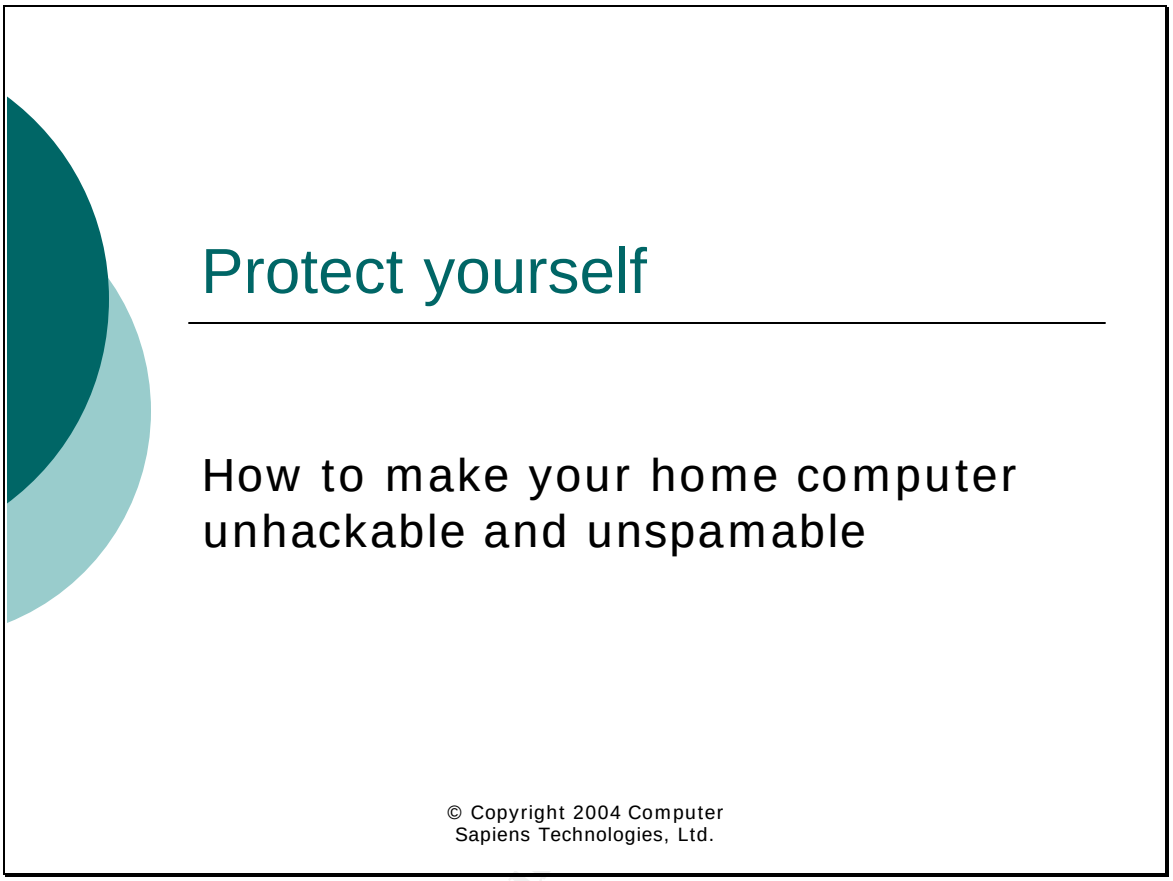
Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec



Title: How to Make Your Home Computer Unhackable and Unspammable: a Computer Security Course for Home Users

Author: Yury Sabinin

Computer Sapiens Technologies, Ltd.

Submitted for GIAC GSEC certification September 7, 2004 under GSEC Practical Requirements v. 1.4b

This material is intellectual property of Computer Sapiens Technologies, Ltd. All rights are reserved.

Any qualified person or entity is authorized to use this material to deliver in-classroom training, provided that:

1. The material is unmodified and unedited, except the name of the trainer in the introduction chapter
2. No charge, direct or otherwise, is made and no monetary or other material benefit is expected
3. Computer Sapiens Technologies, Ltd. is notified by mail or e-mail of the course delivery using this material

For any other use, written permission from Computer Sapiens Technologies, Ltd. is required.

For any questions regarding the material, or to make suggestions or corrections, to notify Computer Sapiens Technologies, Ltd. of a course delivery, to request permission, to request PowerPoint slides, or to clarify acceptable use and qualification guidelines, contact:

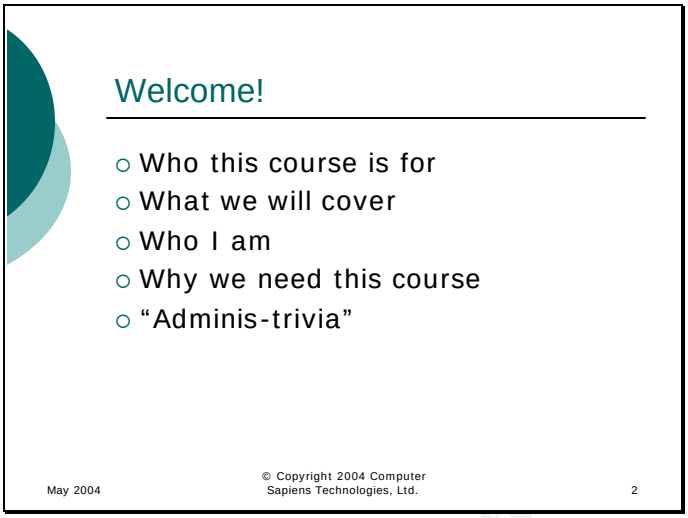
Yury Sabinin

President,

Computer Sapiens Technologies, Ltd.

yury@computersapiens.net.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

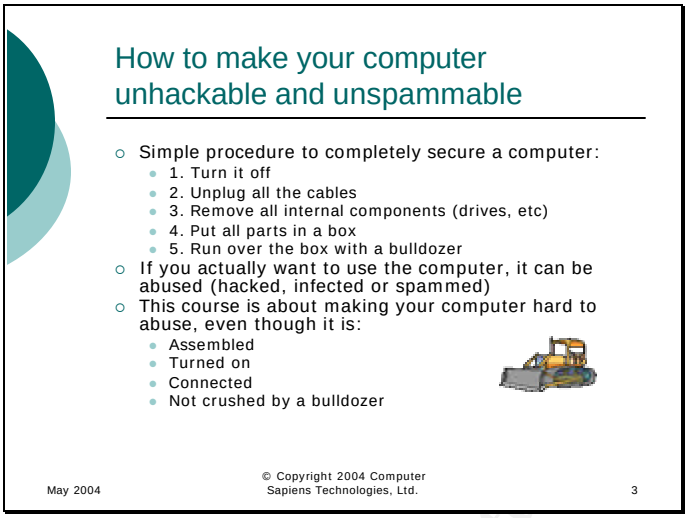


Welcome to the “How to make your computer unhackable and unspamable” seminar!

In the first part of this course, we will go over what this course is about, who it is for, why it is necessary from your perspective and the perspective of the security professionals who already know all this stuff, and, of course, how the day is going to unfold.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

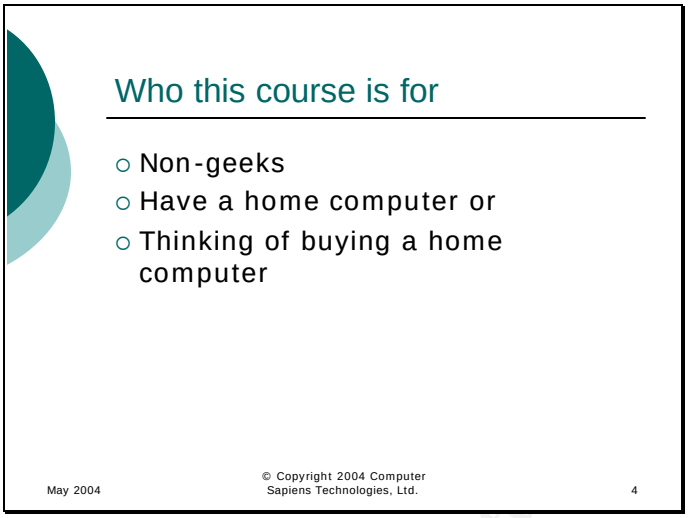


OK, maybe the course title promises something that cannot be achieved without taking extreme measures. If a computer can be used, it can also be misused. If you can read e-mail, some of it will be spam. If you can get at your data, so can someone else who is good at convincing the computer that they are you or that they should have access to the information. The only way to prevent your computer from being misused is to physically destroy it.

However, in most cases, we are not looking for making the computer absolutely, totally unhackable (although sometimes that is the requirement – for example, hard drives for some law enforcement agencies are physically ground into dust when the computer is taken out of service). We are going to talk about how to make a computer easy to use but harder to misuse – a compromise most of us are interested in achieving.

There is a widely held belief that all computers lie somewhere on an infinite line between total usability and total security. Total usability means anyone can use it for any purpose imaginable; total security means no one can use it for any purpose at all. We are aiming for the point where you can use it for all purposes you need it for and no one else can use it for purposes that do you do not approve of. For example, you can use your computer for checking e-mail, and no one else can use it to gather information about you or to launch attacks against Microsoft or Red Hat.

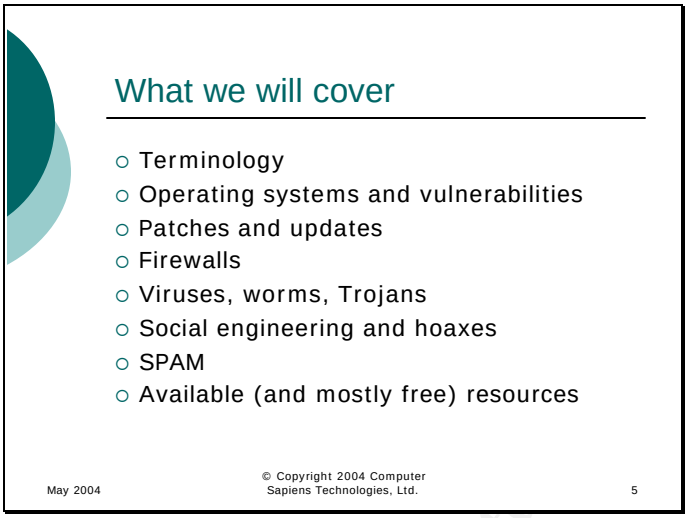
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



There are, of course, many books and courses that deal with hardening computers and networks against just about any threat imaginable. The problem is that they are mostly aimed at computer professionals or at least people with a thorough knowledge of computer technologies and an interest in learning the intricacies of computer systems. The problem is that most of the computers "out there" are in private hands, and the people who own and use them have priorities other than learning the details of operating systems, hardware, and other components – they just need the computers to satisfy their need for news, entertainment, connect to their families in other cities, or look up the TV channel grid for the day. Let us face it – computers are only tools, and us people in the "computer field" often forget about that.

This course is designed for a home user, not computer professionals. Many of the things in the course would be obvious to a professional geek, and none require any knowledge of computers other than being able to turn one on and use the keyboard and mouse. However, you will be amazed how easily you can protect your system and defend against most viruses, attacks and scams. If every home user takes the steps we are going to discuss, life will become very difficult for cyber-criminals!

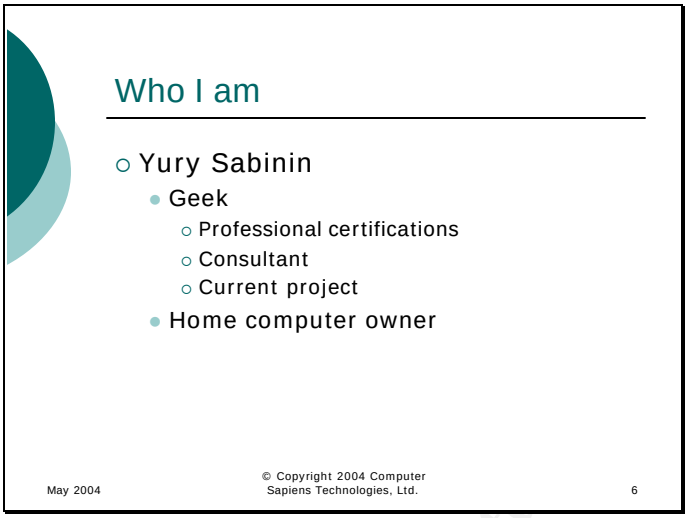
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



During this seminar, we will cover the most common threats out there – viruses, trojan horses, spam, scams and other activity unscrupulous people use to try and get at your money, steal your identity, or just make a personal statement. We will not get into defending against a professional hacker going specifically after your computer – that is for computer professionals to deal with. However, professional hackers are unlikely to go after your system – they are more interested in secret data belonging to companies and governments. The people you and I need to defend our home systems against are amateurs, vandals, small-time crooks – and what we need is to harden our systems just enough to make automated tools fail. This is like putting a lock on your house's front door – it will not stop a professional (who is not interested in your home, anyway – do you have a chest of diamonds under your bed?) but will likely keep you safe from 99.9% of the "small fry" that is looking for a quick hundred bucks and does not mind lugging a 32'' TV to a pawn shop to get it.

For each "Chapter", we will first get familiar with the terms used in the industry to describe common concepts. The chapters themselves will deal with the threats that you are facing each day – viruses and other "unfriendly" software, cons, spam, as well as basics of your computer and how to make it criminal-resistant. A special emphasis will be on the resources you have at your disposal – mostly for free.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



My name is Yury Sabinin. I am a computer professional, and have been working with computers for more years that I should really admit to. I currently take care of some of the most secure systems for a very large global company. In short, I am a geek.

I have achieved professional certifications from Microsoft, Oracle, IBM and Cisco, well-known software and hardware manufacturers. I am currently working on GSEC, a well-known (in computer professional circles, of course) security certifications from The SANS (SysAdmin, Audit, Network, Security) Institute.

I act as a consultant when necessary and own Computer Sapiens Technologies, Ltd - and I also have a full-time job for a large multinational company as a security manager. But most importantly, I am also:

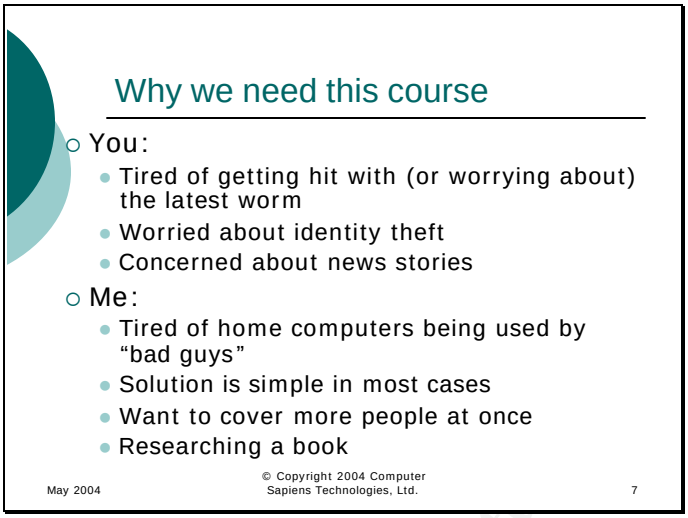
A home computer owner!

It is a totally different ball game at home. I can no longer justify tens and hundreds of thousands of dollars for specialized security hardware and software. On the other hands, I don't have data that would be worth billions of dollars if accessed by unauthorized people. I can't spend all my time working on my home computer's security – on the other hand, I do not need to. I cannot try to prevent every possible attack at home because the computer has so many different functions, unlike the single-purpose systems I deal with at work. On the other hand, the people I am trying to keep out of my home system are very different from the people I am trying to keep out of the systems at

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

work. My work is almost irrelevant to this course – today I am speaking to you as a home computer user, not a security professional.

© SANS Institute 2004, Author retains full rights.



In the many years I have been a "computer guy", I have had countless questions from friends, neighbours, relatives about how to protect their computers, or how viruses work, or what to do when you get "hit" with one, or is an e-mail about a virus that no software can detect for real or a hoax, etc. Those questions were sometimes sparked by a news story, or a real virus infection, or many other events– but the problem seemed to be that many people were not aware of the real (and false) threats out there and what they could do about them. There simply is not a lot of easy-to-read, coherent information for the home users. Every antivirus software company and every operating system manufacturer tries to present some good information, but somehow it is either hard to find, or is not well-suited for a starting point. Also, people always prefer a live person to explain a concept to them for the first time rather than having to read it online. In this course, I hope to give you the starting point and the "Big Picture" so that you can use the great many other sources to continue learning as much as you need about protecting yourself from unfriendly cyber-elements out there. In reality, all the steps we will discuss here are simple, common-sense things no more complex than remembering to lock your front door.

I also have another agenda which is hopefully shared by my colleagues in the computer security field.

It is well known that the home computers are being used by the "bad guys" to launch powerful attacks against the systems we protect as professionals – so doing my part in helping home users defend their machines makes my job as a security professional

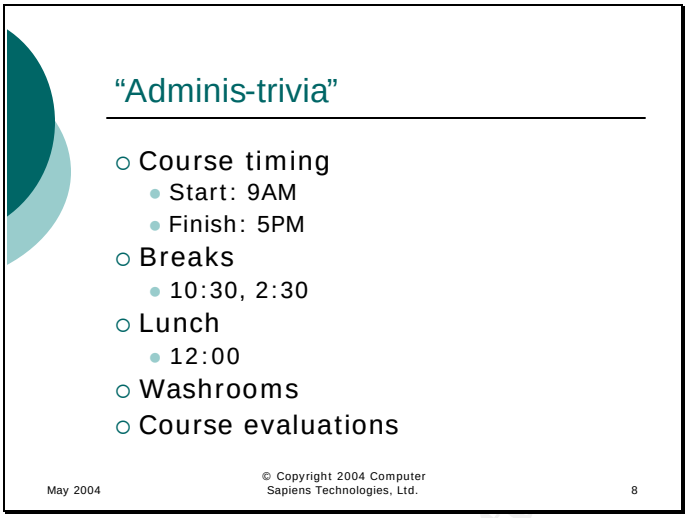
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

easier, one classroom at a time. Licensing this course for free delivery by other computer professionals helps more. It also lets me answer questions for more people at a time, especially since the answers are often more simple than people expect and the questions are more common than most of us realize.

In addition, I am considering writing a book for the home users on how to protect their computers. This course may serve as the foundation for that book in the future.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

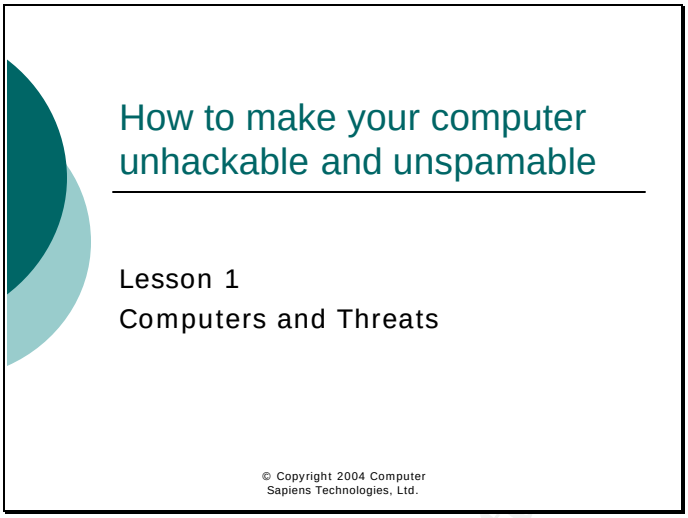


Timing of this course may vary for each class. The times above are the usual, expected guidelines.

Course evaluations are handed out at the end of each class. They are optional and anonymous but help me greatly in continuously improving the material and delivery.

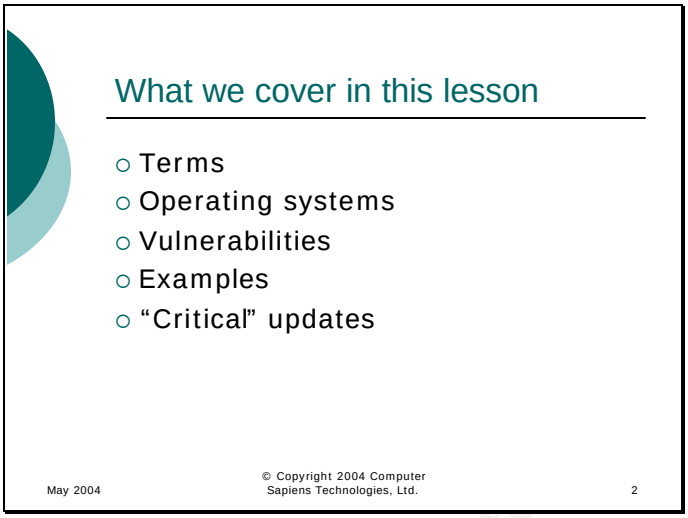
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

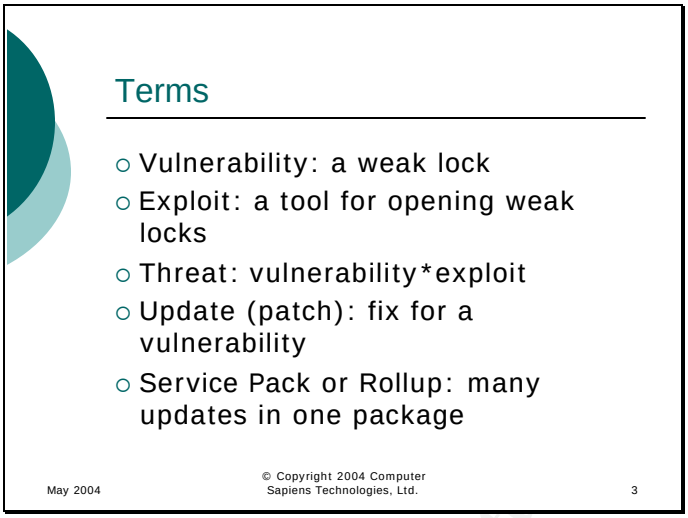


You turn on the news – there is a new virus out there wreaking havoc on companies' networks and home users' PCs. You open a newspaper – there is another bunch of hackers trying to attack another government's site using home users' machines as zombies. You go to a water cooler – there is another know-it-all talking about how operating system X is safer than operating system Y. How do you make sense of all of this? What is true and what is not? How do you stay ahead of all of these things?

In this lesson, we will cover some of the terms used in the industry (and often misused in the press), talk about some of the most common operating systems and discuss the concepts of threats and vulnerabilities. Most importantly, we will introduce the concept of regular system updates, especially the ones the software manufacturer considers "Critical".

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



First, some terms. The easiest way to understand them is to make an analogy between your computer and your house. Both are your private territory, both contain valuable stuff, and both are exposed to the outside world that contains some unfriendly elements. Both need to be protected.

A vulnerability is a security weakness in the operating system or one of the applications running on your computer. For example, a vulnerability may be a bug in the browser that allows a web page to read the contents of your drive without your permission. A vulnerability is similar to a weak lock: it is not really dangerous until it is known, and it does not cause any harm until someone takes advantage of it.

In order for a vulnerability to become a real rather than a potential problem, it needs to be exploited. In the above example, an exploit is the web page that actually reads the contents of your hard drive without your permission. Using the house analogy, an exploit is the special tool that can be used to easily open your vulnerable lock.

A threat exists when there is a vulnerability discovered in your operating system or one of the applications you are using and a practical exploit for that vulnerability has been created. Using the house analogy, there is a threat when you know that you are using a weak lock and you saw the special tool sold at the flea market down the street, so you know that some bad guys may be able to open your door any time.

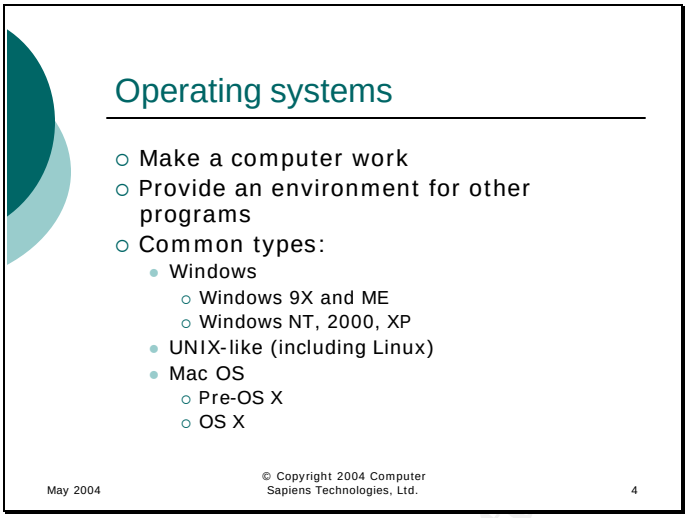
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

An update is a small program that fixes the vulnerable operating system or application to eliminate the vulnerability. It is easy to apply and usually does not change the functionality of your applications, just fixes whatever bug was causing the vulnerability. It is similar to replacing the lock or just the cylinder inside it so that the special tool the bad guys have no longer works on your door.

Finally, a service pack or a rollup is simply a number of updates combined into a single package to make them easier to apply and to create a known baseline for your system – for example: “Windows XP Service Pack 2” – if you tell a professional that this is your operating system, they will know that all of the updates in the Service Pack 2 have been applied to your system and you do not need to worry about them. Service packs sometimes do include new features or change the functionality of your system. For example, Service Pack 2 includes a much more powerful software firewall than the one included with the original version of Windows XP.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



When a company builds a computer, it is just a piece of hardware that contains all the right parts but cannot do anything yet. In order for a computer to work, it needs software that manipulates all those parts (reads and writes data from the hard drive, uses the video card to put graphics on the screen, etc). That is the function of the operating system. The operating system is the basis for all of the applications you normally use (e-mail, word processor, web browser) and provides them with the interface to the hardware and an environment to work in.

The reason that the operating system is very important is that it is the common ground for all of the programs on your computer. If there is a vulnerability in one of the applications, only that application is affected; if there is a vulnerability in the operating system, it can affect the entire computer.

There are numerous operating systems available for the home users. The most common are Windows, Linux and Mac OS. It is very important to know which system you are running, so that you know which vulnerabilities you need to be to be alert for.

Most home PCs run some version of Windows. There are two “families” of Windows – the versions that originated from the Windows 3.X and Windows 95, and the ones that evolved from Windows NT. The former include Windows 95, Windows 98 and Windows Millennium Edition; the latter – Windows NT, Windows 2000 and Windows XP.

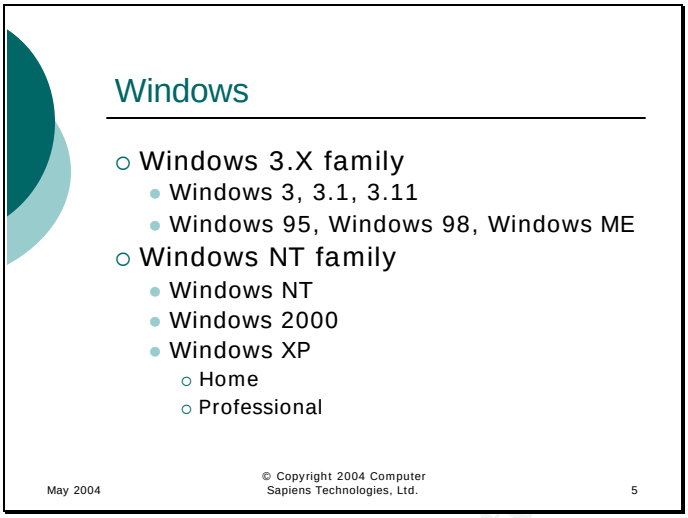
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

UNIX-like systems are a lot less common among home users, but from time to time they show up pre-installed on new computers or even just hard drives. Most are variants of Linux, a free UNIX-like operating system.

Macintosh is another fairly popular operating system that only runs on Macintosh computers such as the iMac. There are really two types of MacOS: MacOS 9.X and below, and MacOS X (pronounced “ten”). While the former are proprietary, the latter is actually a UNIX-like system underneath a proprietary interface.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Since most of the home computers run one of the Windows versions, let us discuss Windows in a little more detail.

The oldest common family of Windows is the Windows 3.X. You would be running one of these versions only if you have a very old computer. It is no longer supported by Microsoft, so it would be impossible to keep it current with security updates. If you are running a computer with Windows 3.X on it, it is time to upgrade – you have definitely got your money's worth out of that one!

After Windows 3.X, the same basic operating system evolved into Windows 9X, including Windows 95, then Windows 98, and finally, Windows Millennium Edition (ME). Although they look much better and are a lot more functional, they share the same problems that the original Windows line had – they are not designed with security in mind. They are also a lot less stable than the Windows NT family of Windows. Although Windows 98 and Windows ME are still supported by Microsoft, Windows XP (the current version of the Windows NT line) is a much better choice. If your computer is fast enough to upgrade it to Windows XP, it is well worth the money.

The other line of Windows is the Windows NT family. Unlike the Windows 3.X/9X line which were all just interfaces on top of DOS, the actual operating system, Windows NT is the actual operating system which includes powerful security features and was designed for corporate use and for use with sensitive data. It is unlikely that a home user would be running any version of Windows NT prior to Windows 2000, the point

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

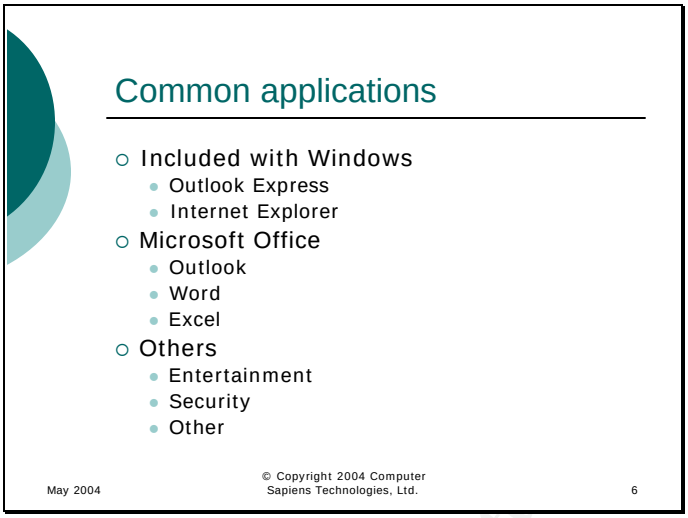
where Microsoft started promoting this family for home use. The current version of Windows NT (and the only version of Windows Microsoft currently sells) is Windows XP.

Windows XP is a very stable, robust system with good backward compatibility with Windows 9X applications. It is actively promoted and maintained by Microsoft, and the support for it is going to be available for many years to come. It comes in two flavours: Home and Professional. While for a computer specialist the Professional version is a must, its added capabilities are unlikely to be used by the average home user and therefore do not justify the premium you would pay for the upgrade from Home to Professional.

No matter which operating system you have, make sure that you can still get the security updates for it from the manufacturer's site. Otherwise, it is time to upgrade.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



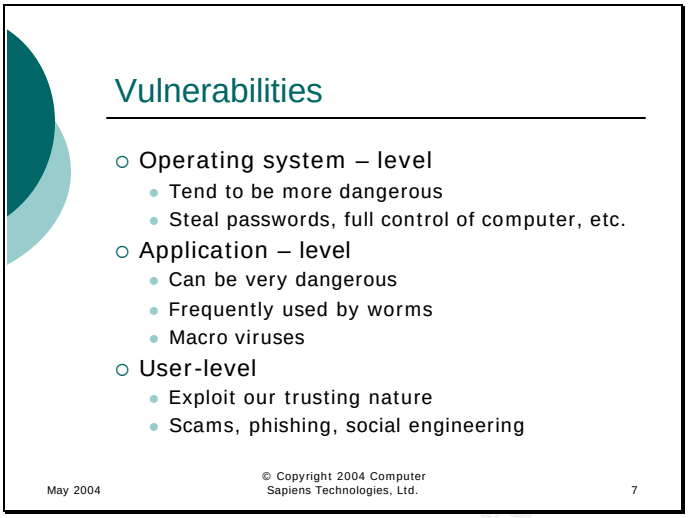
What you usually use on the computer directly is not the operating system itself but rather applications (programs) that run on it.

Some applications are included with the operating system and generally come pre-installed on your computer. The most common ones are the e-mail client (Outlook Express) and the web browser (Internet Explorer). Although they are bundled with the operating system and in some ways can be considered part of it (the operating system relies on them for some of its functions), they are still separate applications for our purposes.

Some others are installed separately. The most common suite of applications that is independent of the operating system is Microsoft Office. It includes a word processor (Word), a spreadsheet application (Excel), an enhanced e-mail client (Outlook) and, depending on the "edition" of Office, other applications such as the Access desktop database engine.

There are, of course, other applications that you can use for entertainment (games or music player), security (antivirus programs), financial management (Microsoft Money) or other purposes.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Both the operating system programmers and the application programmers are human and, therefore, can make mistakes or fail to foresee some unusual situation and how their program would react to it. As the result, both the operating system and the applications that run on it have vulnerabilities, or weaknesses that can be exploited by malicious people or software.

The vulnerabilities at the operating system level tend to be more dangerous because they lie at a more fundamental level of your computer and are capable of affecting more of its functions, including “innocent” applications running on top of the operating system. Using an operating system vulnerability, a hacker can steal passwords by logging your keystrokes, or even take complete control of your system.

Application – level vulnerabilities can be just as dangerous but are generally (not always) limited to the scope of the application. For example, a vulnerability in Outlook Express is more likely to allow an attacker to access your address book than let him format your drive. However, tighter integration between applications and the operating system blurs this distinction, because an average application has more capabilities to be exploited.

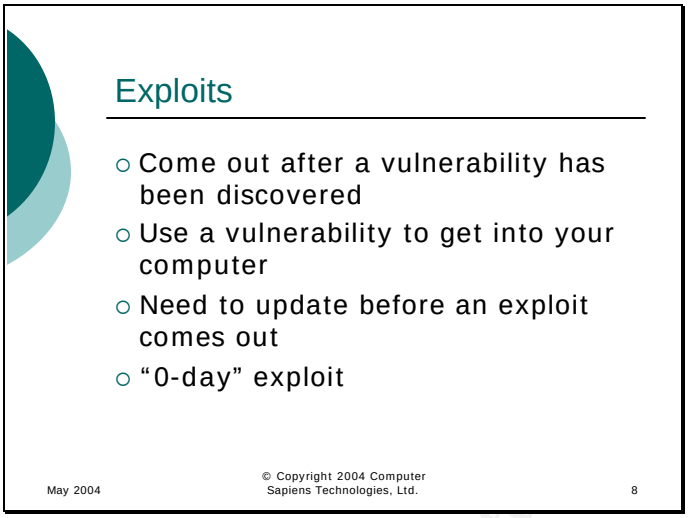
Although not usually discussed in the vulnerabilities sections of security books, one of the biggest vulnerabilities that affects us all is our trusting nature. This vulnerability existed well before the computers, and has been exploited for just as long by various scam artists.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Most of the malware use application-level or user-level vulnerabilities to infect your computer, although some (like Sasser) use operating system “holes” and do tend to cause a lot more “noise”. If you see a bunch of geeks look at their pagers, mutter something and run out of the room – there is a worm that exploits an operating system vulnerability hitting their company’s network.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



An exploit is a practical way to utilize a discovered vulnerability for malicious purposes.

As a rule, an exploit uses a known vulnerability because the people who find "holes" in the systems and applications tend to be researchers, not criminals. However, once the vulnerability has been discovered and disclosed, it is only a matter of time before some criminal comes up with a practical way to use it for his or her purposes, usually in the form of a worm.

The best way to defend yourself against exploits is to make sure that by the time it comes out, the vulnerability it uses to penetrate into your computer has been fixed by applying the latest patches from the software manufacturer. Since most of us use Microsoft products, patching them is especially important because a vulnerability in one of the products that runs on 95% of the desktops is more likely to get exploited that one that exists on only the other 5%- what is the point of creating an exploit that only works on the computer of some old guy in Southeastern Russia?

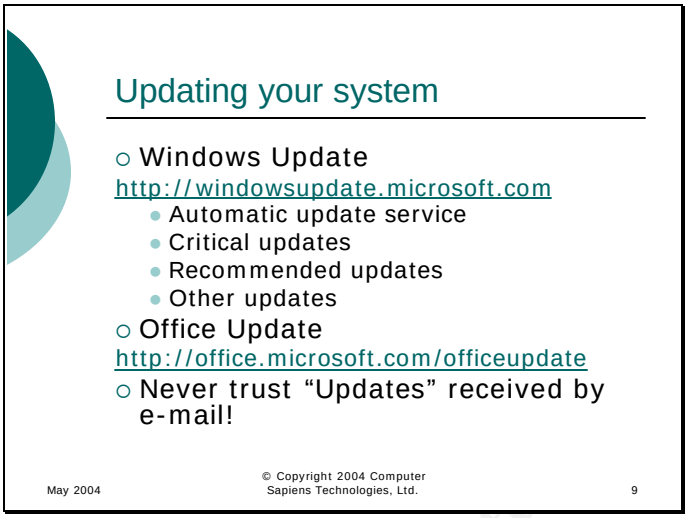
The worst possible scenario is an exploit that uses a vulnerability that has not been previously discovered and therefore has no patch to fix it. An example (although not on a very large scale) is the recent "scob" code. It is a script that was placed on a few web servers that places a key logger on the computer of the users who visit the infected web sites. However, the exploit did not get written into a self-replicating worm but seemed to be placed on the web servers manually, which limited its damage. Had it used a previously unknown vulnerability to spread, it would have been extremely difficult to stop

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and would have likely infected an extremely large number of computers before anything could be done to stop its spread.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Although vulnerabilities in software are unavoidable, it is very important to patch them before exploits for them become available. Basically, we need to stay one step ahead of the thugs that write the malicious code, so that when a worm comes knocking on our doors, it is too late – the vulnerability it exploits to get in has already been fixed.

Keeping a Windows system up to date is actually very simple and does not take any time at all, thanks to the Windows and Office update sites and the Automatic Update feature in the operating system (although not available in Office yet).

To check your system for security ("Critical") updates that need to be applied, just go to the Windows Update site. You will be surprised how many updates need to be applied the first time you go there, but after you apply all the updates that should have been done a long time ago, the list will become a lot shorter – and most of the time, you will see the satisfying "You do not need any updates" message.

To make keeping your system up to date even easier, Microsoft introduced the Automatic Update feature for Windows. All you have to do is select to have the updates downloaded or even applied automatically, and your computer will periodically check the Update site all by itself, download the updates and either notify you or even apply the updates automatically.

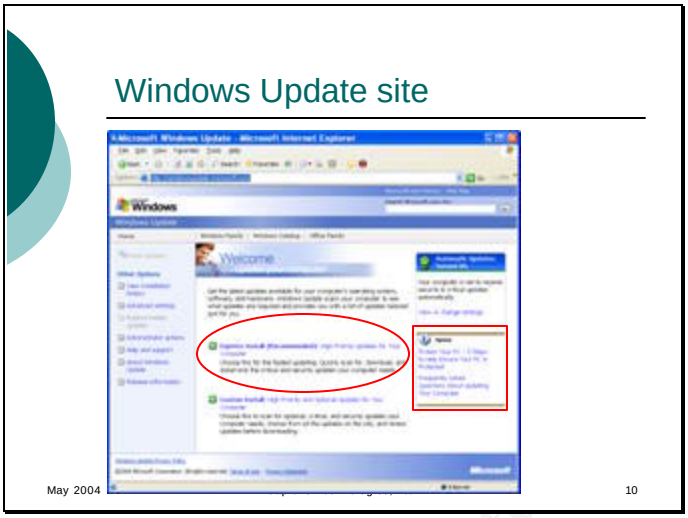
One very important thing to keep in mind: never, ever trust an update that arrived in an e-mail, even if you trust the person who sent it. If it is a legitimate update, it will be on

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the update site – if not, your friend has already been deceived and now your well-meaning friend is sending you something you really don't want on your computer.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



When you visit the Windows Update site, the site will determine which version of the operating system you are using and which updates have already been applied. Once your computer is scanned, the site will determine you which updates still need to be applied.

All updates are classified into High Priority (Critical) and Optional. For security, you need to make sure that all of the Critical Updates are applied. The easiest way to achieve that is to use the Express Install option to allow your computer to automatically download and install the critical updates. If you also want to look at the Optional updates (enhancements to some of the components of the operating system or newer versions of included applications such as Media Player), choose “Custom Install.

On the right, you see that there is a box saying “Automatic Updates Turned On”. If your computer does not have automatic updates configures, in that space you will see instructions on how to enable that feature on your computer.

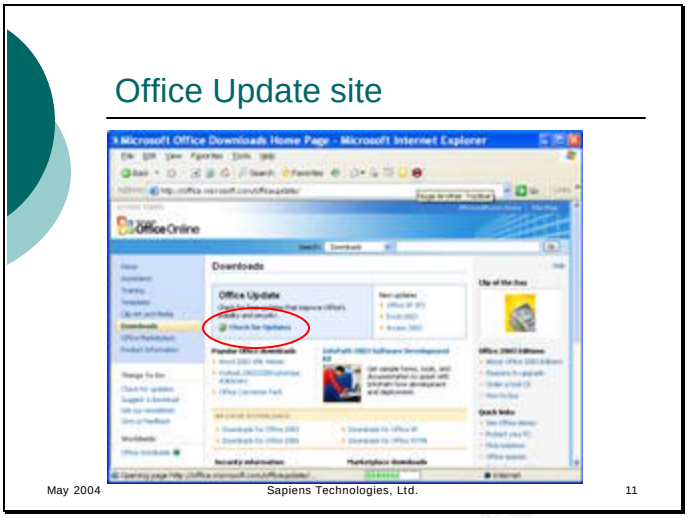
Also on the right, you will see links to excellent and easy to read articles about keeping your computer safe.

After applying the updates, you may need to restart your computer – so make sure that you save any documents you are working on before you start. You may also see that some updates need to be installed separately – make sure that after such an update is applied, you return to the Windows Update site.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

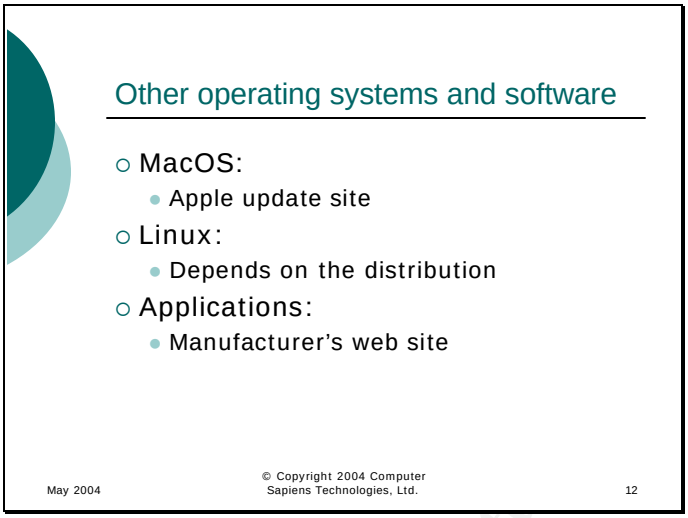
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



The Office Update site is similar to the Windows Update site. It also scans your computer for components (Microsoft Office applications) and automatically determines which updates still need to be applied. However, there is no automatic update feature for Office, so you need to remember to revisit this site every few days.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



For operating systems other than Windows, keeping the system up to date is no less important, although it is a little less user-friendly.

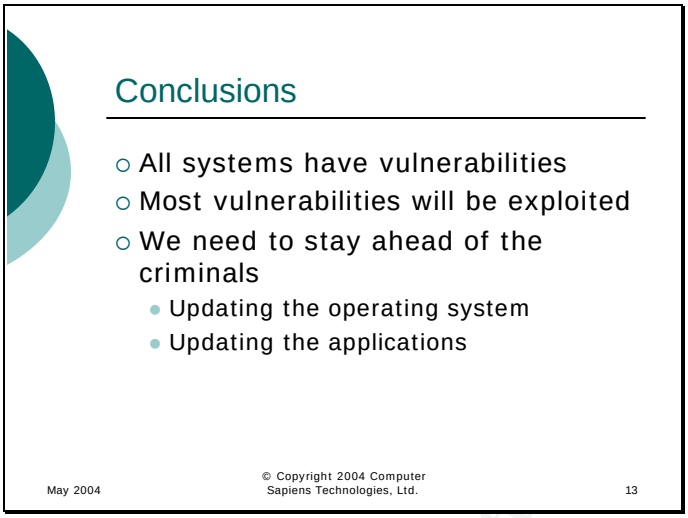
For security updates and information on MacOS, go to the Apple Security website: http://www.info.apple.com/usen/security/index.html

With Linux, you should go to the web site of the manufacturer you bought or downloaded the distribution you are using. There are many distribution of Linux and therefore it would be impossible to list them all here but here are the major ones:

Red Hat: the easiest way that is recommended by Red Hat is to use the Red Hat Update Agent (up2date) .
SuSE: http://www.suse.com/us/private/download/updates/index.html
Mandrake: http://www.mandrakesoft.com/security/advisories

For applications other than Microsoft Office that was discussed earlier, you should check the application manufacturer's web site for any updates.

© SANS Institute 2004, Author retains full rights.

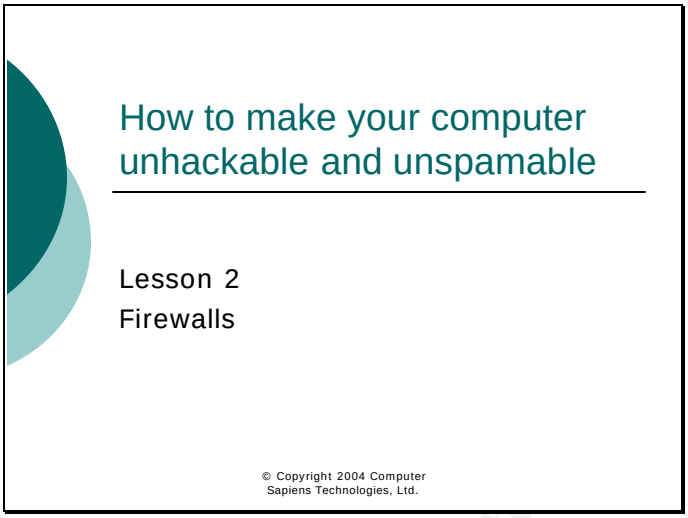


As you see, all systems and all applications have vulnerabilities, some of them discovered and others still unknown. When a vulnerability is discovered, the software manufacturer will generally try to create a fix for it because it is just a matter of time before someone comes up with an exploit for it.

Our strategy should be staying ahead of the exploits by applying updates that the software manufacturer supplies on their web site or through an automated update service as soon as they become available.

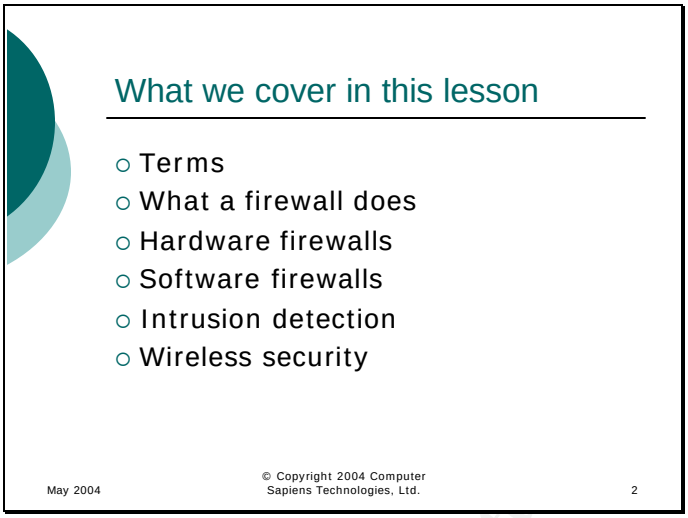
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

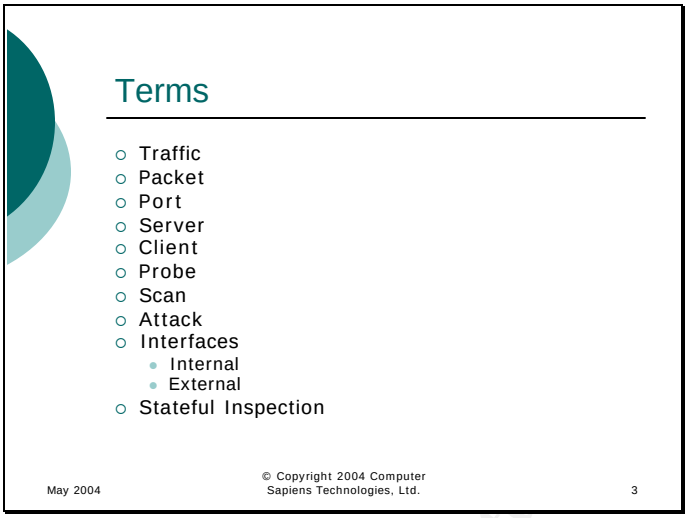


In this lesson, we will discuss firewalls. Although it sounds like a scary, technical term, firewalls have got a lot more user-friendly in the recent years – and also came down in price. These days, there is little excuse not to have your computer protected from attacks by a hardware or a software firewall.

We will now spend some time discussing some of the common terms we will be using throughout the lesson, the benefits of firewalls and then we will get into the difference between software and hardware firewalls, benefits of using each of them, and then we will talk about related technologies – intrusion detection and wireless networking.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



First, some of the terms that we will need to understand for this lesson.

Traffic – a stream of data that comes to or leaves your computer.

Packet – computers send data in portions called “packets”. Each packet has a source and a destination, and can be analyzed by firewalls to determine whether it should be allowed through.

Port – a virtual address of a process on your computer. Any application that needs to use the network to communicate will use a unique port. By knowing the port a packet is addressed to, we can find out which application the packet is trying to reach. If a port is “open”, your computer is accepting incoming packets on that port.

Server – a computer that is providing services to other computers by waiting for and responding to incoming requests. Any computer can be a server, and most home computers are by default configured to be servers in some respects.

Client – a computer that is using the services of a server. Most home computers are primarily clients – they are using the services of web servers to browse web pages, and the services of an e-mail server to send and receive e-mail.

Probe – a special packet designed to find out whether a port on your computer is open, making it potentially vulnerable to an attack.

Scan – a series of probes to common (or even all) ports on your computer designed to find open ports that can be used for an attack.

Attack – an actual attempt to hack your system or make it unable to communicate.

Interfaces – the network cards that are connected to a network. In case of a computer, there is usually only one; hardware firewalls usually have two or more.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

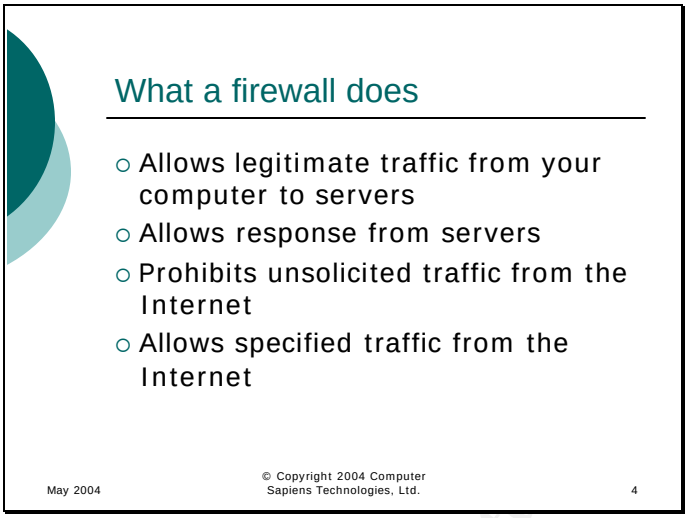
Internal Interface – the interface on a firewall that is connected to your internal network and therefore your home computer.

External Interface – the interface on the firewall that is connected to the Internet via an ADSL or cable modem.

Stateful Inspection – a firewall technology that examines the packets going through it and tries to "understand" not only their source and destination, but also what type of a packet it is.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



A firewall is a program or a dedicated hardware device that all the traffic between your computer and the Internet passes through. It examines the packets that go both ways and decides whether the packet should be allowed through or not. In order to do that, the firewall must be "taught" what is safe to allow and what is not.

When you buy a firewall, it is usually preconfigured for the common applications to work without any changes to the firewall configuration. For example, a request from your web browser to a web server will be allowed through, and so will the response from the web server back to you. However, an unsolicited packet from the Internet (for example, a probe or a port scan) will be stopped by the firewall because it does not "remember" you asking for that packet.

This configuration is a good start – it allows you to initiate any communication with the outside world and to receive a response. It will allow web browsing, e-mail, and any other Internet-aware application most of us use.

However, sometimes we need to allow other traffic to pass. For example, you decide to check out the peer-to-peer sharing networks where people share music, digital videos and other files. Peer-to-peer networks can be dangerous places and require other users to be able to access your computer to get the files you want to share, so by default a firewall will not allow a connection. However, if you really want to join such a network and accept the risks, you can configure the ports the network needs to be open to be "forwarded" to your computer. That means that when a packet arrives to the firewall that

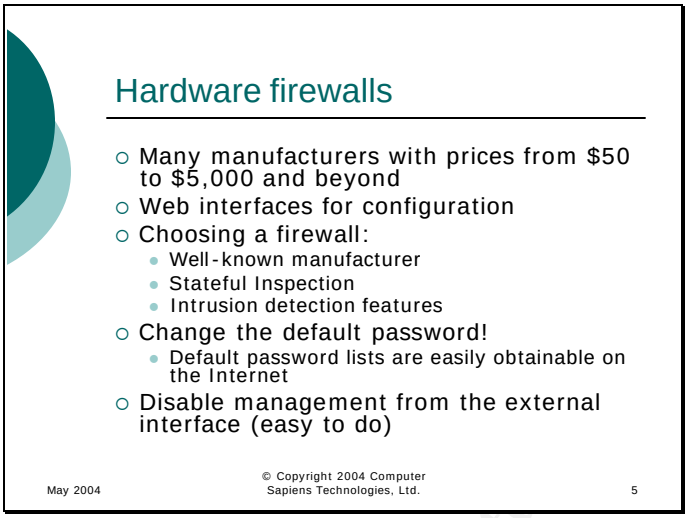
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

is addressed to the port the peer-to-peer network uses, it will be forwarded to your computer instead of being dropped. This makes your computer a server in addition to being a client – that is the idea of peer-to-peer networks.

Some firewalls base their decisions only on the source, destination and port number. Others try to look inside the packet and evaluate its contents in order to figure out whether the packet is part of a legitimate conversation, whether the contents are harmless or are some kind of an exploit. These “smart” firewalls are called Stateful Inspection Firewalls. It is a good feature to have when you are buying a hardware firewall.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



There are many makes and models of hardware firewalls on the market today. Some are designed for home use and cost under $100, others are for large corporations and can cost thousands of dollars. For a home user, there are absolutely no advantages to running a business-class firewall: it has a lot of features you do not need, a lot of configuration options you will never use, and can handle the amount of traffic you will never generate. So, let us concentrate on the firewalls designed for home use.

All of the newer firewalls these days have a very easy-to-use configuration, with web interfaces and even wizards that walk you right through configuring it for the first time or changing the configuration later. Manufacturers of firewalls realized a long time ago that no matter how good a firewall is, if it is not configured properly, it is quite useless and may even be dangerous by giving the user a false sense of security.

You can go to any computer or electronics store, or even some drug stores like London Drugs in Canada to buy a home hardware firewall. Try to buy a firewall at a bigger retailer who offers a good return policy if you are not satisfied for any reason (for example, you find the interface hard to navigate).

Choose a well-known manufacturer such as Linksys, DLink, NetGear or SMC. Just like with any other purchase, do some research in advance – talk to your friends who have firewalls, look for user reviews on the Internet, etc. Talk to the sales clerk and ask which model was returned less often than the others. For example, a model that was returned

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

by 50% of buyers may be one to avoid – it is either too hard to configure, or it may have some design flaw (for example, it overheats easily and stops working).

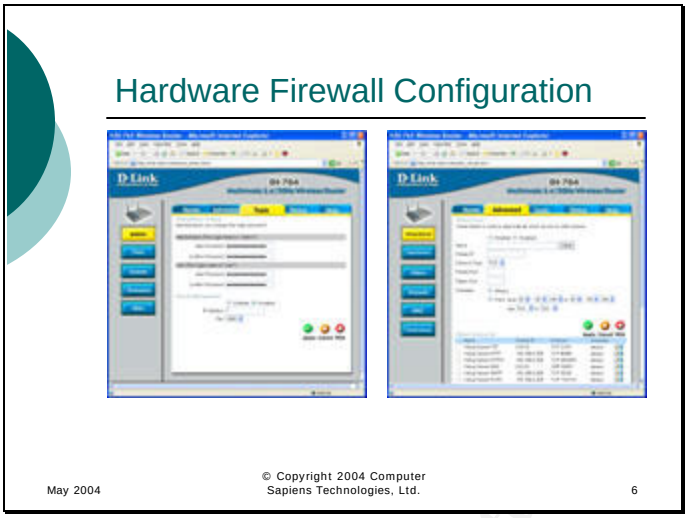
Compare the features of different firewalls you see on the shelves. Stateful Inspection is good to have, and so is Intrusion Detection (more on Intrusion Detection later). Some firewalls may have other features such as a built-in printer port so that you can share your printer between computers, or a built-in wireless access point. Only consider those additional features if you need them and do not pay extra for the features that are of no use to you. Look for a firewall that has a very easy configuration program – a wizard is best if you have never used a firewall before.

Once you buy the firewall and bring it home, read the instructions and follow them closely. Make sure that you change the default password – the Internet is full of default password lists, and if you do not change your password, it is very easy for an intruder to start managing your firewall and make it wide-open to all traffic. If the firewall allows this (and most do), disable management connections from the external interface. This means that an intruder would not be able to configure your firewall from the outside and you can only configure it using one of the computers on your own network.

Once that is done, you will be able to use your computer to do everything you used to do without the firewall – but much more safely. If something that you used to use does not work any more, you will need to do some research on how to make it work. Usually, the manufacturer of the software you are having problems with has a step-by-step guide on configuring a firewall to allow their application to work. As a rule, it requires forwarding one or more ports to your computer.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



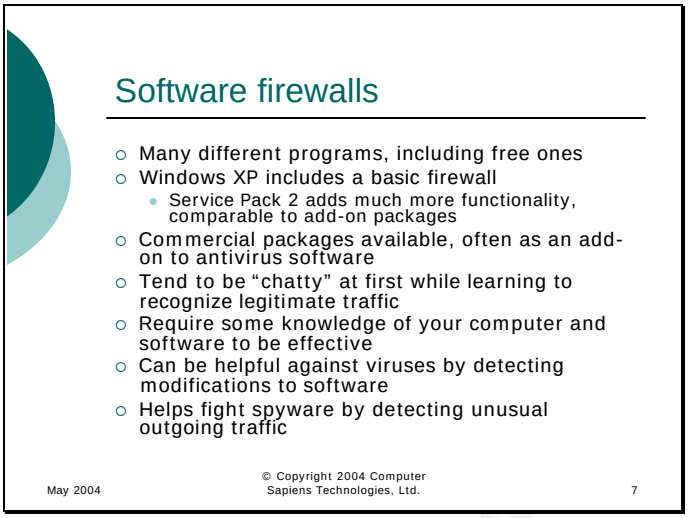
Above you see two fairly typical screens from a web interface of a hardware firewall.

On the left, you can see the screen that allows you to change the administrator (and, in this case, user) password on the firewall. On the same screen (may be different on another firewall), there is the option to enable or disable remote (external) management. With Remote Management disabled, you can only configure the firewall from the internal network, providing another layer of protection from an attack.

On the right, you see the configuration screen for the “port forwarding” functionality of the firewall. Although it does look fairly complex, you are not really expected to know how to fill it in by yourself: an application or online service that requires ports to be open will generally tell you which ports need to be forwarded to your computer from the firewall. Most home users would not need this functionality unless there are teenagers in the house who enjoy online gaming.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



You can also install a program on your PC that acts as a firewall but does not require a separate device – those programs are known as "software firewalls". There are many such programs, many of them free. An example of an excellent free software firewall is ZoneAlarm from www.zonelabs.com.

Windows XP included a very basic software firewall when it first came out. When you upgrade to Service Pack 2, the firewall functionality and configurability will expand tremendously and almost start approaching some add-on software firewalls in many respects, although it still is weak on client application integrity and behaviour checks.

There are also commercial software firewalls. Most often, they are bundled with antivirus products as "Security Suites". They are available from such antivirus vendors as Symantec and McAfee.

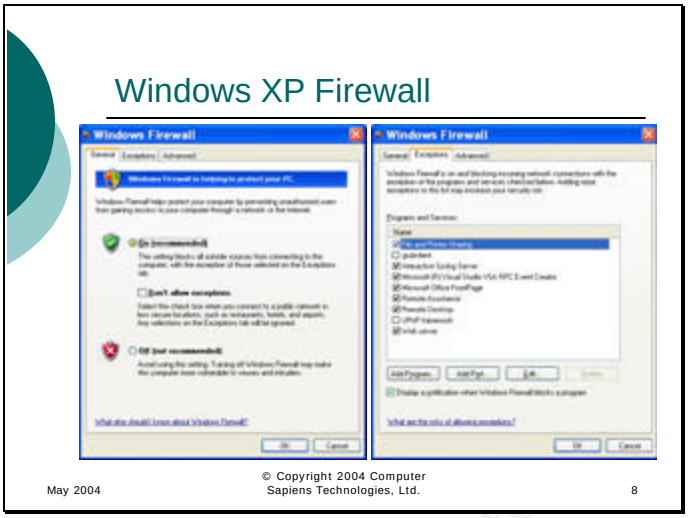
Software firewalls work by learning what is acceptable traffic and what is not. They are generally preconfigured to allow web browser and e-mail traffic and to ask the user whether to allow any other type of activity. Once you give them the answer, they remember it and do not ask the next time the same traffic is encountered. Because of this learning process, most software firewalls tend to be "chatty" in the beginning and get a lot quieter after the initial period is over. However, many firewalls also "fingerprint" the applications on your system to guard against modifications made by viruses. If an application you allowed to communicate changes in any way, the firewall will ask you again whether to allow it to communicate or not. If the modification was intentional (you

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

applied an update to the web browser), you would allow the firewall to save the new fingerprint and allow access; otherwise, you should get very suspicious.

In order to use a software firewall, you need some knowledge of your computer and software that runs on it – otherwise, you will just end up answering “yes” to every question it asks and will get no real protection. However, because of the fingerprinting ability of the software firewalls and its ability to detect which application is trying to communicate, it may be effective against some malware that either modifies existing programs or tries to send data to an attacker.

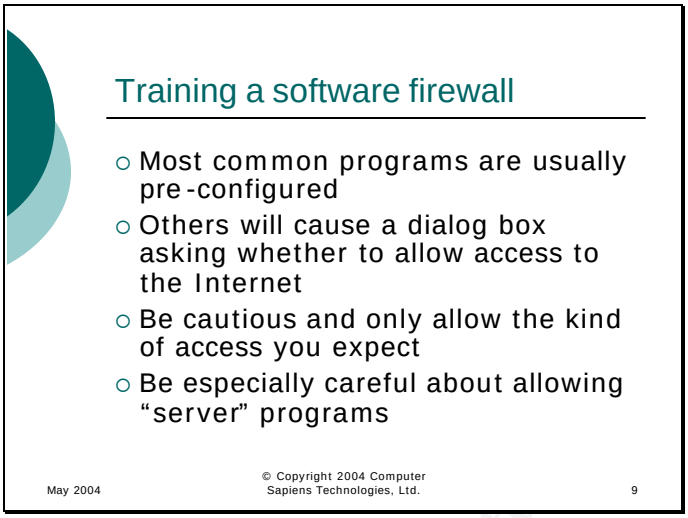
© SANS Institute 2004, Author retains full rights.



The Windows XP Firewall (Service Pack 2) is shown in this slide. On the left, you see that the firewall is enabled – it means that your computer will drop all unsolicited incoming packets except the ones that are allowed on the “Exceptions” page on the right.

The “Exceptions” page shows services that are allowed to accept incoming requests. If you are only using a software firewall and not a combination of software and hardware firewalls, you should not allow any exceptions at all. You can check the “Don’t allow exceptions” box on the General tab (on the left) to completely close the firewall.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

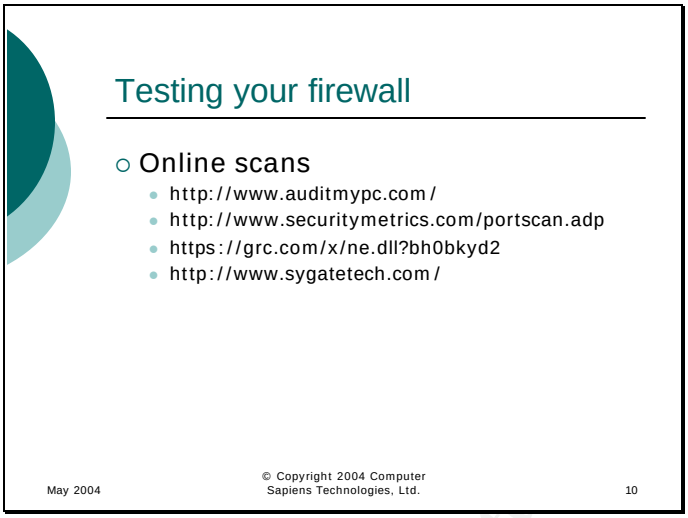


When you install a software firewall, it examines your computer and allows the applications that it recognizes to access the Internet. Other applications are set to "Ask" by default – when an unknown application tries to access the Internet or to open a port to allow inbound access, the firewall will bring up a pop-up box asking you whether to allow the access or not. If you recognize the application as legitimate, you should allow access. If not, it is likely to be a spyware application or a backdoor trojan.

There are two types of access an application can attempt: outbound (client) or inbound (server). In the case of outbound access, the application is trying to communicate with a server on the Internet. The danger is that the application may be spyware sending sensitive information into the wrong hands. In the case of inbound access, the application is trying to become a server and allow outsiders to access it. This may be a trojan (we cover them in the next lesson) opening your computer to a remote attacker.

© SANS Institute 2004, Author retains full rights.

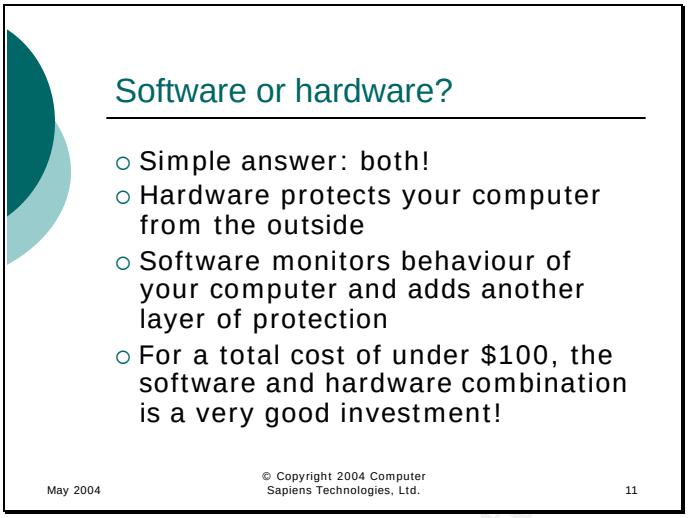
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



There are a number of free sites that can check whether your software or hardware firewall is effective. They all work more or less the same way – you go to the site, agree to not sue the company for scanning you and getting the information on you (none of the companies will sell any of it or use it for any purpose, but make sure you read the agreement anyway) and click a “Scan Me” (or similar) button. In most cases, you are looking for the “Stealth” result which means that your firewall is quietly dropping the packets, without even giving any indication that your computer is there at all. Without a firewall, your computer would have sent an error back, revealing its presence and possibly inviting an attack.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



So, should you use a software of a hardware firewall?

The ideal case is both. Although they perform the same basic function, software and hardware do it so differently that you want to combine the strengths of both in order to get the best protection for your computer.

The hardware firewall is going to protect your computer from external attacks. Although a software firewall is supposed to do the same thing, there are viruses that attempt to turn off the firewalls, leaving you exposed – a virus cannot do that to a hardware firewall because it is an independent device. Also, a hardware firewall does not annoy you with pop-up messages until you start answering "Yes" to everything – and that happens often with software firewalls.

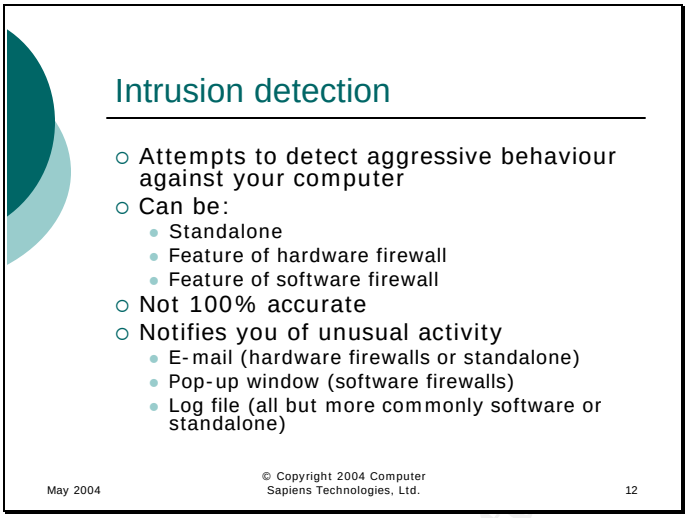
However, a software firewall is in better position to monitor programs that run on your computer, detect changes in them and inform you when a program is doing something unexpected. In general, home hardware firewalls allow all access from your computer to the Internet – a software firewall can be configured to only allow certain programs to access it, preventing some spyware from sending the data it gathered. Also, if your hardware firewall is compromised, the software firewall will add another layer of protection. This is very important if you have a wireless network access point built into or attached to your hardware firewall.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Since there are good free software firewalls and hardware firewalls are now well in the under-$100 range, there is no reason not to have both.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Intrusion Detection is an old technology that has now made its way even into the inexpensive, home hardware and software firewalls. It attempts to analyze the traffic going to your computer and detect known or even unknown attacks based on either known patterns or simply “unusual” activity that does not fall within what the firewall has come to expect.

Intrusion detection features are present in many of the products available to you: hardware firewalls, software firewalls – and there are also standalone products (software and hardware) that can be used independently of the firewall you have.

Because an intrusion attempt can take many different forms, intrusion detection is not always accurate – sometimes the system will panic when there is no attack taking place (false positive) or it may not notice a skilled attacker (false negative). However, it will generally tell you about the more obvious port scans or attempts to exploit a known vulnerability.

Once an attack has been detected, the intrusion detection system will record it in a log file and will attempt to notify you in any way it can. A standalone hardware system or a firewall with this feature will generally send you an e-mail with the detail of the attack; a software firewall with intrusion detection is likely to show you a pop-up window.

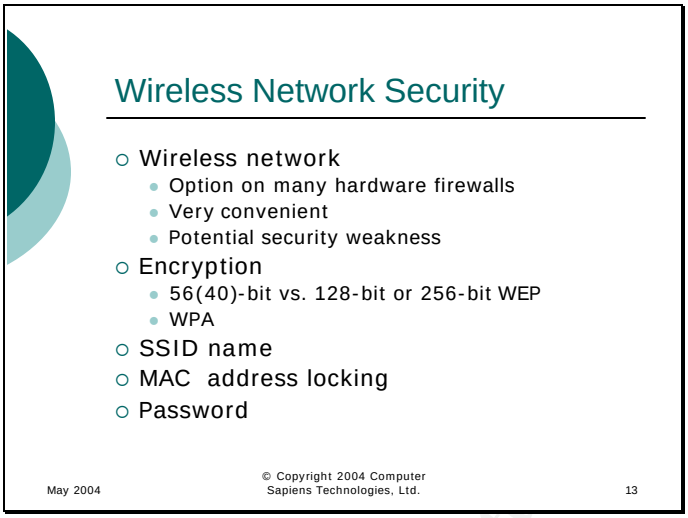
An intrusion detection system does not generally stop or prevent an attack, although many can be configured to take some form of action – for example, to block the address

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

of the computer attacking you – but this defense is activated only after the attack has started. Because of this, you still need to be aware of the patches that need to be applied and use the firewall and antivirus software, whether or not you have intrusion detection in place.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



In the recent years, there has been a lot of interest in wireless networking – and many home users find the convenience of locating a computer anywhere in the house and being able to use the Internet without having a cable snake through the rooms a very appealing concept. Wireless is now built into many laptop computers, PDA's and even some phones. However, the current generation of wireless networks has its weaknesses as well as its many strengths.

If you do decide to enable wireless networking, you need to make sure that you are the only one using your wireless access point and that the data you send back and forth over the air is not easily intercepted. While you are browsing the Web, you may be sending or receiving financial or other private data, you may receive sensitive e-mails, etc – and without encryption, all of that can be very easily intercepted by an eavesdropper. Also, the wireless network is usually located behind your firewall, so an attacker can connect to your wireless access point and have direct access to your computer, defeating the hardware firewall. Given these considerations, you should always enable the highest level of encryption your wireless access point and the cards you use in your computers support.

There are two encryption standards: the older one, WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). WEP has a number of well-known security flaws and is easily broken, regardless of the key length; WPA is more secure. Most of the new wireless equipment supports WPA; some of the older hardware can be upgraded – check the manufacturer's web site. There are experts who recommend that if you are

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

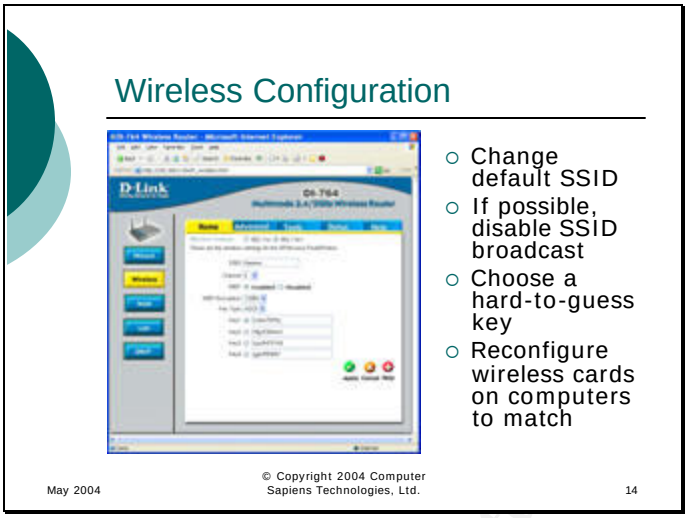
using WEP, you should stick to the lowest key length your equipment supports (40 or 64-bit) because with this protocol, longer keys increase the processing demands and the overhead without offering significantly more protection.

The access point and the wireless network card in your computer use the SSID (Service Set Identifier) to identify the network. The SSID is not encrypted when transmitted, so the only thing that can be done to discourage the eavesdroppers is to change the name from the default and disable its broadcast. If your access point supports disabling the SSID broadcast, you should be able to find the procedure to do that in the user's manual or on the manufacturer's web site.

A feature many access control points offer is to limit communications to specific wireless network cards by using their hardware (MAC) ID. While not bulletproof, this feature adds another inconvenience to an attacker.

Last but definitely not least, just like with any device on your network, make sure that you change the admin password on the access point as soon as you plug it in for the first time!

© SANS Institute 2004, Author retains full rights.

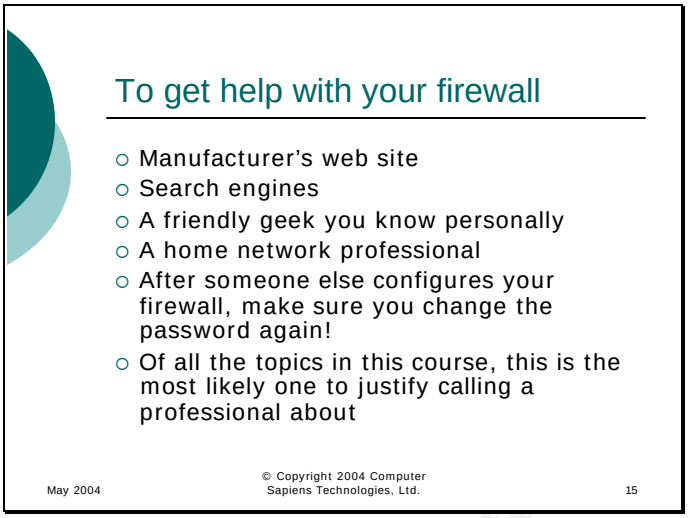


The configuration page for your wireless router or access point should look similar to the one above.

Make sure that you change the default SSID and, if possible, disable its broadcast (this device does not have the option to disable SSID broadcast). Enable encryption and choose a difficult-to-guess key because anyone trying to connect to your network will try 12345, 99999 and other simple combinations. However, do not choose the same number you use elsewhere, especially your bank PIN – the encryption on your wireless network can be broken, and the attacker may attempt to use the key to try and steal your identity since a lot of people use the same number everywhere.

Once the wireless access point or router is configured, you will need to reconfigure the wireless cards in your computers to match those settings before you can connect.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Although the firewalls have become very easy to configure, the importance of doing it right justifies some work. Make sure that you do not guess an answer to a question you may have while setting one up – a wrong guess could leave you wide-open to an attack. Go to the manufacturer's web site – they generally have good FAQ lists. If that does not answer your question, e-mail or call the manufacturer with your question – you are entitled to support if you bought your firewall recently and legally.

You may want to do a quick search engine query – I find it especially helpful when a software firewall asks if some program I am not quite familiar with is asking for access to the Internet. You can type in the name of the program that is displayed in the pop-up and find out if it is legitimate of not before answering the Allow/Deny question.

If you know a computer-savvy person, this may be time to call in the favour he or she owes you (make sure you have good coffee and cookies on hand). If not, you may want to call in a reputable computer professional – this is one of those things that are important enough to pay a few dollars to have it done right.

If someone other than you does configure your hardware firewall, change the password after they leave. No matter how much you trust a person, you would probably not give them your bank PIN, right?

Finally, a confession: configuring a firewall is the one area in this course that is the most likely to generate a support call to a professional – either the manufacturer's support

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

line, or someone who can come to your home and configure the firewalls. Since this does not need to be done regularly, do not hesitate to have someone who knows how to configure a firewall do it for you initially – even if you have to pay for it.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

How to make your computer unhackable and unSPAMable

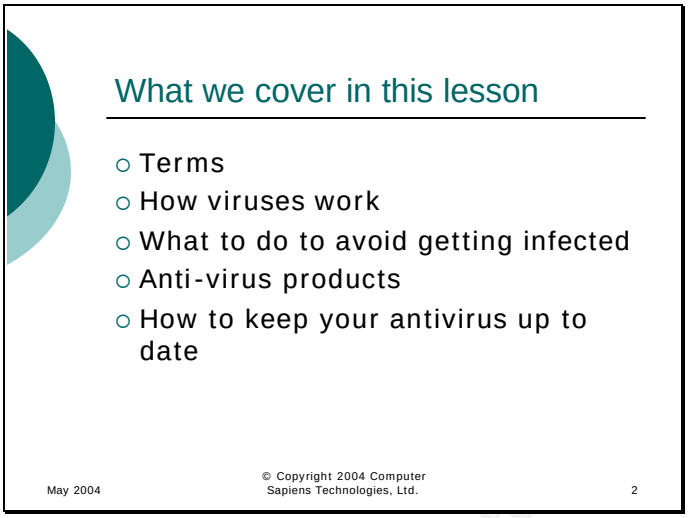
Lesson 3

Viruses, worms and Trojans

© Copyright 2004 Computer Sapiens Technologies, Ltd.

© SANS Institute 2004, Au

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

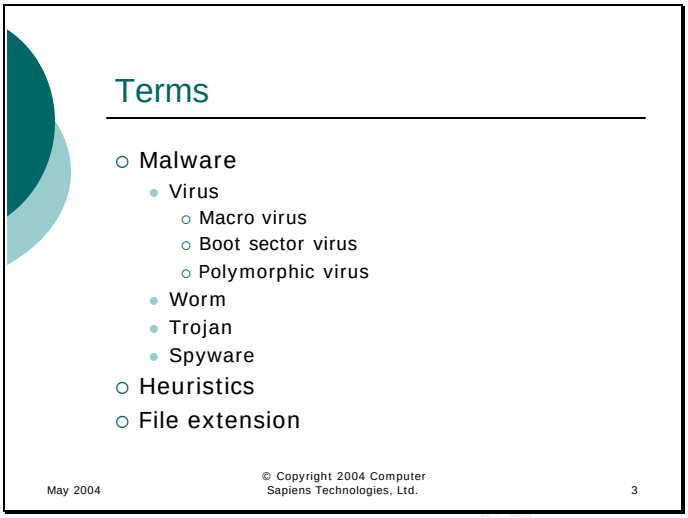


In this lesson, we will talk about a group of programs that fall into the category of "malware" – malicious software. Although the distinctions are often blurred, these programs are classified as viruses, worms and trojans. The class of software known as "spyware" can also be arguably placed into this category, especially if it is installed without your knowledge or consent.

We will look at how those programs work, how they propagate and how to take reasonable precautions to avoid getting infected. We will also discuss simple configurations for antivirus software and making sure that the most recent malware is detected.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



There are two main terms we should define before getting into any discussions on unfriendly programs and how to deal with them.

First, malware. The term stands for “malicious software” and includes everything that can cause direct damage to your computer or data or add unwanted functionality to it. The first part (causing damage) is simple – if a program tries to delete your music files or spreadsheets, that is quite obvious and definitely unfriendly. The second part (unwanted functionality) is sometimes harder to see. For example, how do you know if a program opened a backdoor to your computer, set a password and quietly e-mailed it to its creator? Or that your computer was programmed to attack the United States Government web site on a specific date? How about a program that is sending every key stroke you type, including passwords and credit card numbers, to its creator? Even if a program is collecting information on where you surf and what products you are interested in, it can be classified as malicious if done without your knowledge or consent.

So, malware can be classified into four main categories:

Viruses – programs that you need to run in order to get infected. A virus can be a standalone program (for example, a game that has been infected on and infects other applications you start afterwards), or a document that has a macro (a small program that was designed to simplify and automate formatting or calculations but can be misused), or the boot sector of a floppy disk (more rare nowadays). Some viruses try to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

avoid detection by automatically modifying their own code when infecting a file so that their signature changes and cannot be recognized by an antivirus program– they are called polymorphic.

Worms – usually scripts embedded in an e-mail or a web page, although many also actively scan networks for unprotected computers. The defining characteristic of a worm is that it does not require you to explicitly run it – it will activate itself using an operating system or program vulnerability.

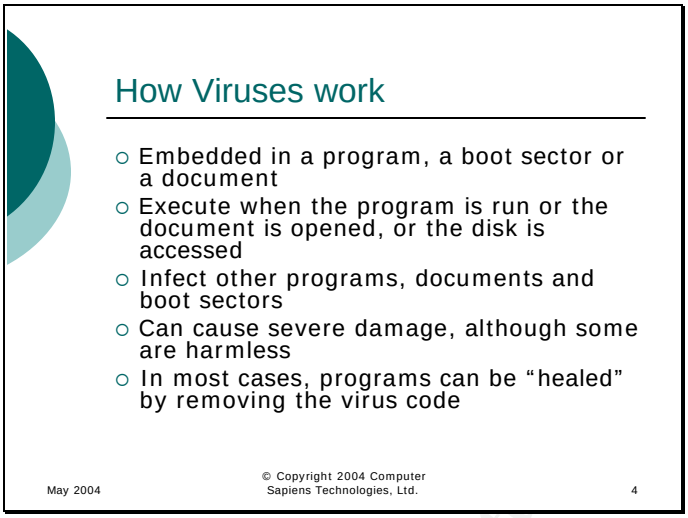
Trojans are defined differently in different sources. Sometimes the definition is unwanted functionality in a seemingly useful program, sometimes it is limited to programs that open a backdoor to your system allowing the author control over your computer. Either way, definitely aggressive. A trojan needs to use some method of propagation and is usually "dropped" by a worm or embedded into an application like a virus, except it does not normally infect other applications the way a virus would.

Spyware is a hot topic right now, and whether it is malware or legitimate software seems to depend on whether you are fully aware of what data is being gathered and whether you gave consent to it. It is being installed on users' computers by malicious web sites without their knowledge, but it is also sold to people who want to monitor what their kids are doing online.

When a virus comes out, antivirus companies quickly analyze it and create a "signature" that can be used to detect it. This signature is then included into the next release of the antivirus software. In order to also detect viruses that have not been "fingerprinted" yet, or viruses that modify themselves every time they run (polymorphic viruses), antivirus programs can try to detect unusual, virus-like characteristics of a program without actually recognizing it as a specific virus. This analysis is called heuristics.

Finally, file extensions. In many operating systems, the computer knows what kind of file it is dealing with by the letters after the last dot in the file name. For example, document.doc has the extension "doc", and document.exe has the extension "exe". Although both file names are "document", the first is really a document and the second is actually a program masquerading as a document.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Although the first self-propagating program in history was actually a worm, the first type of malware to actually become well-known was the virus– that is why most malware is often lumped together as viruses. The reason the virus enjoyed this "golden age" in late eighties and early nineties is that most computers were not connected to the Internet, so the easiest way to propagate a malicious program was to infect a file that users would share – a game, or the boot sector of a floppy disk.

Just like a real virus, a computer virus needs a carrier – a program, a document or a floppy disk (or a hard drive). The virus appends its code to the carrier so that it is executed when its carrier is called – the program run, or the document opened, or the floppy read. When the virus executes, it can do anything it wants – but it usually also copies itself into the memory of your computer and waits there for you to call another file it can infect. If you do (open another document or run another program or insert another floppy), the virus appends a copy of itself to that file, infecting it, as well. If you share that file with someone else, they will become infected, too.

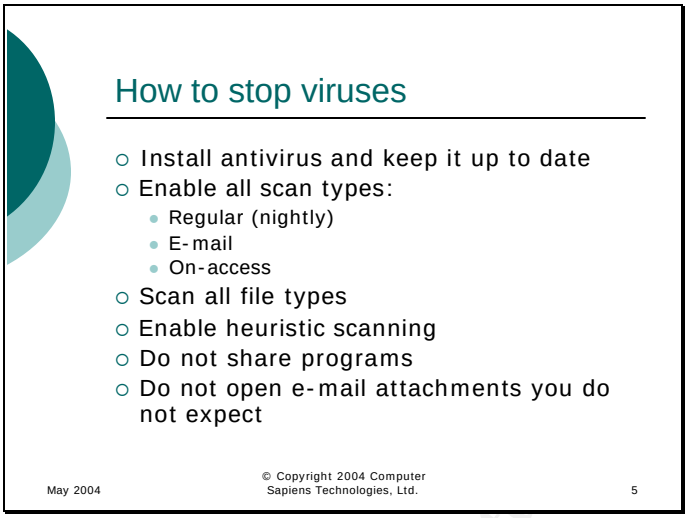
Some of the more recent viruses also attempt to disable the antivirus software running on your computer and software firewalls to avoid detection.
A virus is capable of causing tremendous damage – for example, by wiping most of your files the Michelangelo virus). Some are harmless jokes – for example, your screen gets turned upside down, or a message comes up asking for a cookie and does not go away until you type the word "cookie" (the "Cookie Monster" virus). Because of their propagation methods (manual sharing of files or floppies), they spread quite slowly and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

may take months or years to propagate to a large number of computer users, giving the antivirus companies a lot of time to release new signature files that include the new virus. Infected programs can usually be healed by removing the appended virus code.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



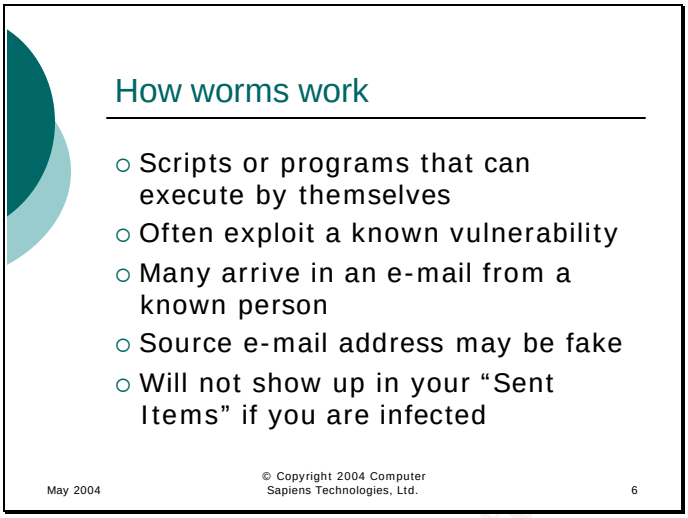
The easiest way to protect yourself against viruses are:

- Install an antivirus program and enable boot sector scanning, on-access scanning and macro virus detection.
- Enabling heuristic scanning helps detect unknown and polymorphic viruses.
- Keep virus definitions updated regularly (daily is best).
- Do not share programs. For free programs, always download them from the site of the publisher; for others, make sure you are using original, licensed CD's.

If you are not expecting an attachment from someone, do not open it. Even if you are expecting a file, it is safer to save it to the hard drive, scan it for viruses and only then open. The same procedure works well for downloaded files.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Recently, most malware that makes the news has been of this variety. The "advantage" of the worm is that it can actively seek new targets and therefore propagation rates are very high. In fact, we have reached the point where new worms can spread so fast that they actually slow themselves down by overloading the networks they need in order to propagate.

Most worms propagate by exploiting a vulnerability in the operating system or an application (such as Outlook), so that a user does not need to actually run an infected program in order to execute the worm. It may be enough just to preview an e-mail, or visit a malicious web page, or even simply have file sharing enabled on the computer when there is an infected machine on the network. There are even worms that exploit vulnerabilities in programs you did not know you had because some programs come as part of others.

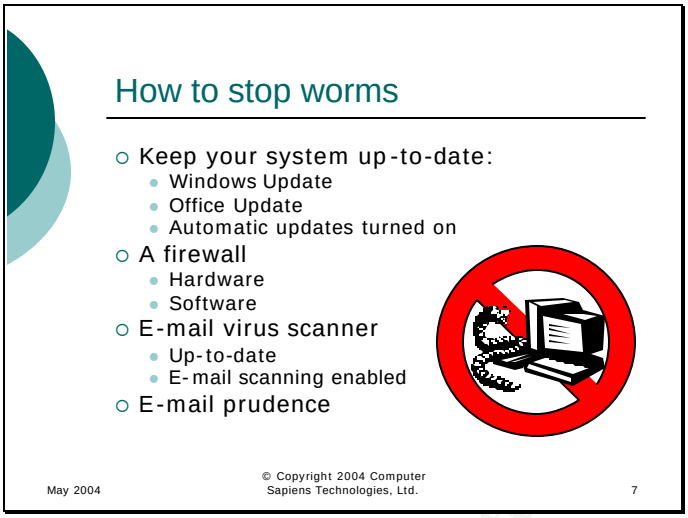
Many worms that spread by e-mail read your address book and mail themselves to people whose addresses you have saved there. Sometimes they use your return address, sometimes a random one, sometimes they choose an address of one of your friends from your address book to use as the return address. The problem here is that you may receive an e-mail from your friend who you trust and open it, infecting yourself. Trying to tell your friend that they are infected may be useless as the message may have come from someone else who had both of you in their address book.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In addition, a worm that you sent if you are infected is unlikely to show up in your “Sent Items” folder because they send themselves out without using your usual e-mail program (they carry their own e-mail client).

© SANS Institute 2004, Author retains full rights.

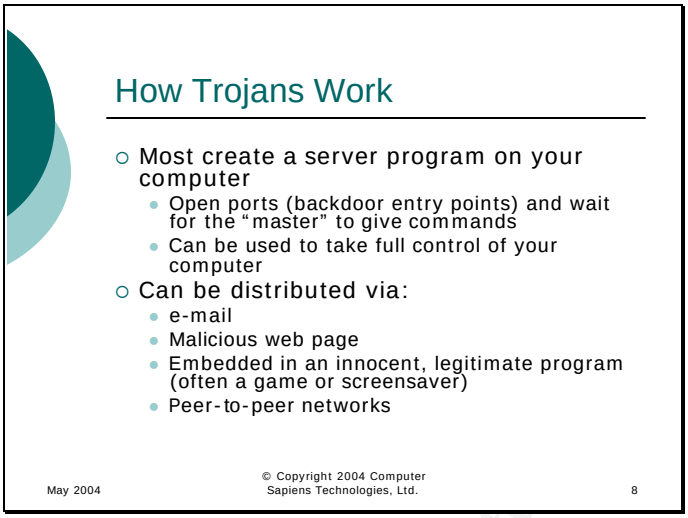
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



To protect yourself against worms, you should take these simple steps:

- Make sure you keep your system up-to-date. Visit Windows Update and Office Update sites regularly and enable the Auto-update functionality in the Windows Control Panel. The most recent versions of Outlook and Outlook Express will block some of the most common dangerous file types.
- Make sure your antivirus software is up-to-date and e-mail scanning is enabled. This way, the attachment will be checked before you can open it.
- Invest in a hardware and/or software firewall. This should block worms that actively look for unprotected and vulnerable computers on the network.
- Be extremely suspicious of e-mail attachments, even when they are sent by (it seems) someone you know and trust. If necessary, verify with that person that they sent you the file. If they did – it probably is not a worm (although it may still be infected with a virus…)
- Make sure that you enable the display of attachment file extensions and check what the extension of the attached file is. Do not click on the “executable” files (.exe, .pif, .cmd, .scr) or scripts (.vbs, .js). Make sure that you look at the entire file name – sometimes the author may insert a large number of spaces at the end the actual file name and before the extension: “document.doc .exe”, making you miss the extension at the end.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



According to strict dictionary definitions, a trojan is a program that has two purposes: a useful one (such as a game) and a hidden one (for example, it allows remote control of your computer by the attacker). Pure trojans do not infect other programs or computers, unless one user shares such a program with another.

Currently, the most common trojans are remote control trojans – they open a "backdoor" to your computer that allows the creator to access your computer with full privileges. Many allow the attacker to manipulate your programs, monitor your keystrokes to steal passwords, credit card information and other useful data, and even turn on the microphone and camera (if your computer has them) and see and hear everything that is happening in front of the computer that is running the trojan.

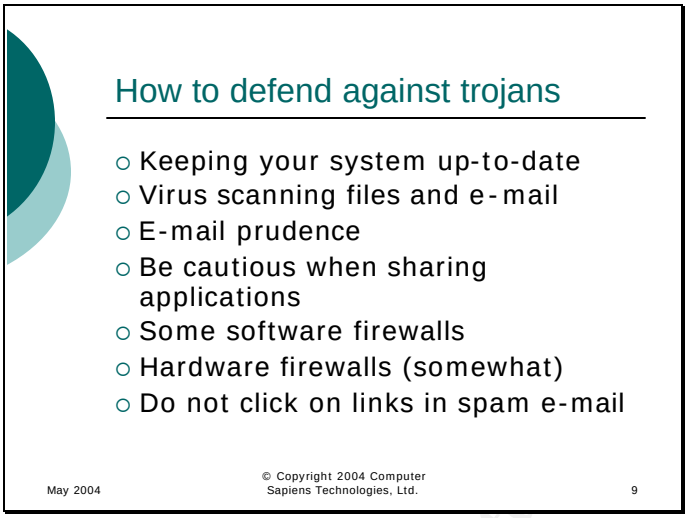
Because of this, the term trojan has come to mean any malicious remote control application or any application that creates a hidden backdoor on your computer to allow unwanted functionality.

Since trojans do not propagate by themselves, they need to be distributed by some other means. The classic, "textbook" trojans are embedded in a seemingly useful application (games or screensavers are common choices). They can also be distributed by a mass-mailing worm that causes your computer to download and install the trojan, or be "dropped" by a virus as part of its payload. Trojans can also be downloaded from a malicious web page, without your knowledge, of course. Most of the time, this method requires the web page to run a script that exploits some vulnerability in your browser.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Another common way for the trojan to get to your computer is sharing files using peer-to-peer networks such as Kazaa or e-Mule. A file that is supposed to be the new hot game can easily turn out to be a trojan.

© SANS Institute 2004, Author retains full rights.

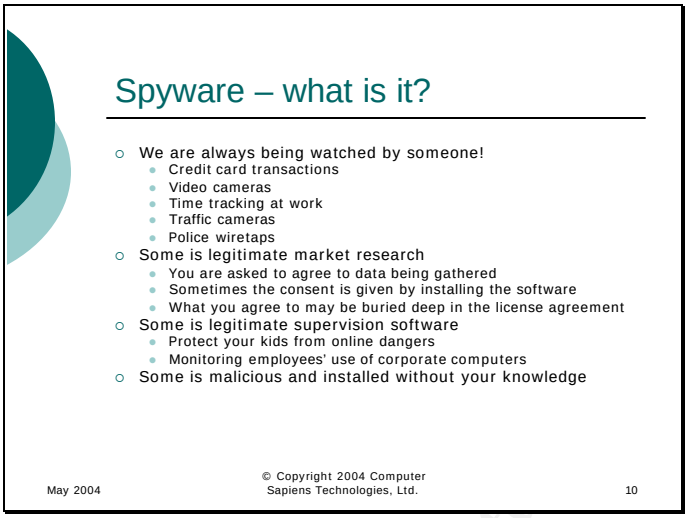


Defense against trojans is similar to defense against other malware.

- Keep your system up to date with all the recent updates.
- Enable virus scanning for e-mail attachments and on-access scanning for all files.
- Make sure that your virus definitions are updates frequently.
- Be very cautious when opening attachments to e-mail messages and any other files received from any source.
- Never share applications by copying them from computer to computer. Always use the original source – for freeware or shareware, the publisher's web site; for other applications, use only original CDs.
- Software firewalls usually detect trojan activity and ask if you want to allow the program to act as a server. If unsure, say "No".
- A hardware firewall will not protect you from a backdoor trojan but it will normally prevent the author from accessing the back door by keeping the port closed.
- If you receive a spam e-mail with a link to what looks like an interesting site, be extra careful – the site may be "booby-trapped" with a trojan, especially if it promises something like free porn, etc.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Whether we like it or not, we are always being watched even when we are far away from any computer. Surveillance cameras are everywhere, time tracking is an accepted form of surveillance at work, traffic cameras can be used to make sure drivers are obeying traffic laws, and all your credit card transactions can be used to profile us all to a very high degree. All of the above have been accepted as legitimate forms of spying on our activities.

Other forms of “spying” require our explicit consent: by filling out a questionnaire to get a free coupon, we agree to having some of our personal information used to improve the marketing of a product.

Then, there is “bad” spying. A wiretap on our phone without our knowledge or a court warrant would be illegal (although it is legal if a warrant is obtained by the police). Someone aiming a video camera at our window, while arguably legal, is not morally acceptable.

Keep this in mind when we discuss spyware. Spyware is just the extension of this surveillance into our online lives. Most of it is legitimate and requires (and gets) our consent. Some is annoying but legal. Some we don’t know about but gave consent to by allowing our governments to pass laws that give the police broad powers of surveillance (I am not suggesting that it is bad, just that it is the case). Some other spyware is the work of criminals.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Spyware is software that gathers information on the behaviour of the user of a computer. It may be logging keystrokes, or even saving screen shots. It may be more or less specialized – from creating a complete log of everything the user typed and did to only gathering information on the user's online shopping habits.

The concept of spyware is far from new. If you think about it, some trojans have a spyware element to them. The difference tends to be that a trojan normally allows the author to observe what is happening on the target computer in real-time while spyware collects the data for later examination and either sends it by e-mail or saves a log file on the computer being spied upon.

Since spyware by itself causes no damage to the computer, it is not inherently malicious. What can make it extremely dangerous is who is using it and for what purpose. What can make it illegal is whether or not you have given consent to having the data gathered.

For example, you may come across a program on the Internet that allows you to add fancy stationery and animated characters to your e-mails. You have seen those e-mails before, and they look really great. Plus, the program is free. You download the program, click "I Agree" to the license agreement (without reading it, of course) and enjoy the fancy e-mail capability.

What you do not know is that in exchange for getting the free program, you agreed to allow the company that provided you with the program to collect data on your online habits. The permission was granted by accepting the license agreement that you did not read and clicked "I Agree" on. As the result, the software is legally installed on your computer.

Another example of legitimate spyware is the kind that allows parents to monitor the use of the computer in order to detect risky on-line behaviour of their kids and help protect them from the dangers that may exist in chat rooms. The same software can be used by a spouse who suspects that they are being cheated on. Some companies may use such software to monitor their employees' use of the computers and make sure that no confidential data is being sent to anyone outside the company.

© SANS Institute 2004, Author retains full rights.

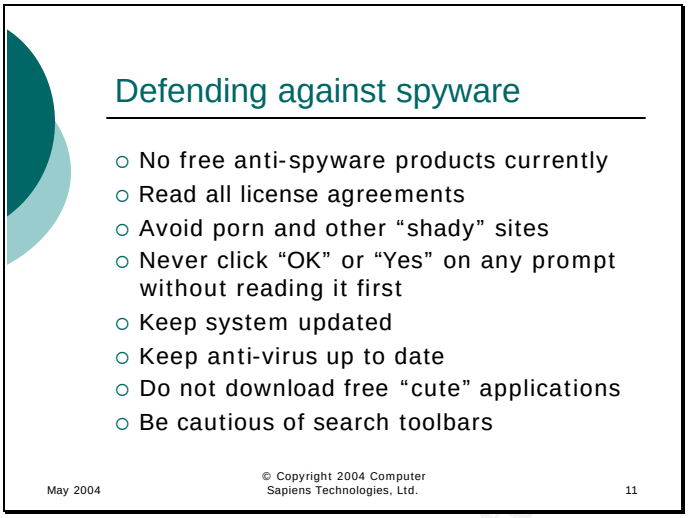
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

And finally, there are programs that are installed completely without your knowledge or consent and do the same thing – gather information on everything you do and send it to someone you do not know. This is both dangerous and illegal. If you go to a web site that requires a log-in, the username and password are sent to the attacker. If you bank online, the card number and online password may end up in the wrong hands. If you buy something at an online store, your credit card information may also be stolen.

The good part is that the spyware of this last class, because it tries to be stealthy, tends to use the same propagation and installation methods as trojans. If you take steps to protect yourself against trojans, you are well on your way to protecting yourself against malicious spyware.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



There are no free anti-spyware products available at this time. Most commercial products offer a free evaluation or demo version that is capable of detecting spyware but will require you to buy the full version in order to remove it.

The way to avoid getting too much marketing and other legitimate spyware on your machine is to read the license agreements before clicking “I Agree”. Although they are written in legalese, you should be able to tell at a glance whether there is a paragraph that grants the software company the right to gather and analyze some information regarding your habits. Keep in mind that the companies that make such legitimate or semi-legitimate spyware try to stay on the right side of the law and are very unlikely to be gathering passwords, credit card numbers and other highly privileged information. However, they may share your purchasing habits with marketing companies, resulting in some direct marketing e-mail coming to your mailbox.

To protect yourself against the “bad” spyware, take the same precautions you would take against trojans.

- Avoid shady web sites – you may pick up a trojan or a key logger without knowing it.
- Most browsers will ask you if you want to download or run a program if a web site tries to send it – make sure you do not click “Yes” without reading the prompt and checking that this download makes sense.
- Keep your system up to date.

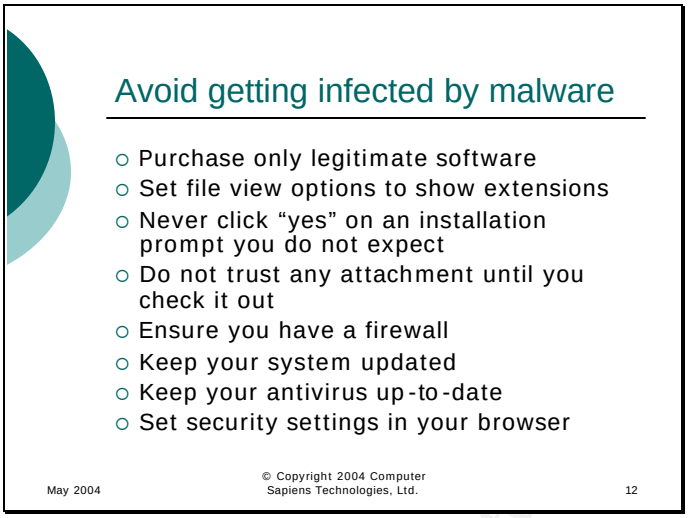
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Update your antivirus regularly. A key logger needs to be dropped on your system by something that may be detected by your antivirus.
- Do you really need that cute stationery for your e-mail?
- A lot of search toolbars have the capability to gather and send a lot of information back to the “parent” site. Be sure yours (if you must use one) comes from a reputable, well-known source.

Finally, if you get an anti-spyware utility, resist the urge to say “Remove all”. You may lose a lot of functionality you have got by agreeing to have some information about you analyzed and used for legitimate purposes. Most anti-spyware utilities will give you a list of spyware detected, including legitimate applications – only remove the ones that you feel are not legitimate.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



You have probably noticed that defense against different kinds of malware is fairly similar. There are only a few simple steps you need to take in order to make an infection a whole lot less likely:

Make sure you know the source of every program you install. For freeware and shareware, use only the publisher’s web site or a well-known, respectable distribution site such as tucows.com; for other software, use only original, genuine CD’s.

Make sure you set the folder options in Windows Explorer to show extensions for all files. This helps catch executable files masquerading as documents, or music, or images.

If a “Do you want to install and run …” prompt comes up at a web page, make sure you know what is being installed.

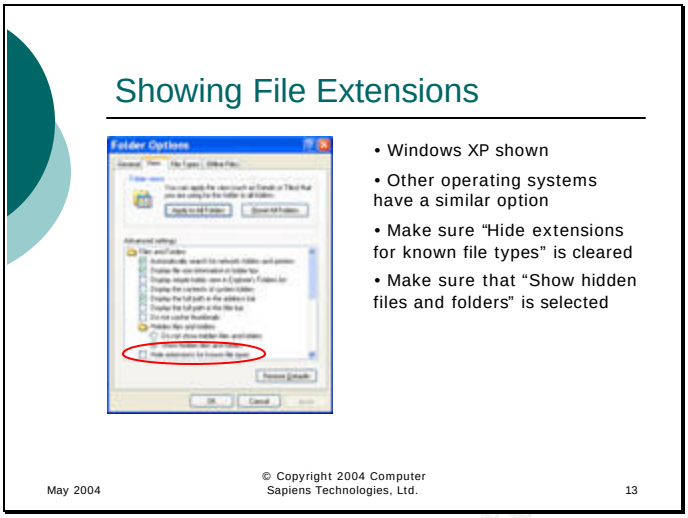
The safest way to deal with an attachment you plan to open or a file you downloaded from the Internet is to save it on the hard drive and check it with the virus scanner before opening it instead of opening the attachment directly.

A firewall is good; two is better. A hardware firewall is harder for a virus to disable; a software firewall is more likely to detect unusual activity on your own computer.

Always keep your system up to date! The amount of time from a vulnerability being discovered to malware showing up is shrinking fast. Enable automatic updates.

Make sure your antivirus software is updated frequently. An out-of-date antivirus is almost useless because these days, it takes very little time from the day a virus is discovered to the day it comes knocking on your door.

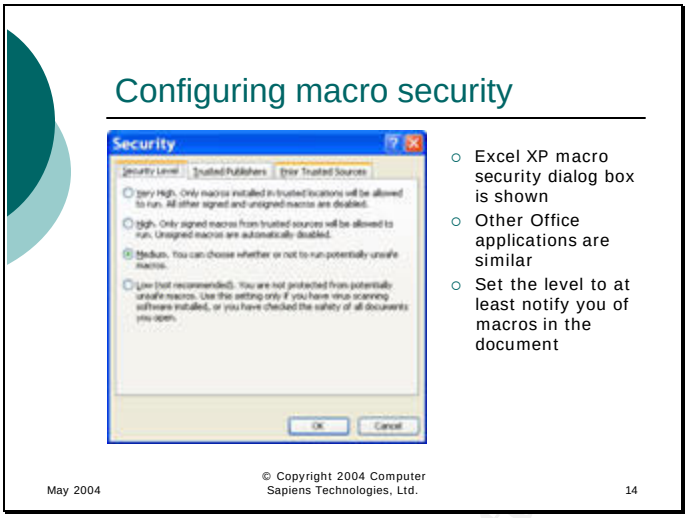
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



To make sure that you see the extensions for all the files and are not fooled by a name like "Document.doc.exe", open Windows Explorer and click "Tools -> Folder Options", or open the Control Panel and double-click "Folder Options". Make sure that the "Hide Extensions for known File Types" is cleared. You should also select "Show hidden files and folders" to make sure that the simple trick of making a file "hidden" cannot be used to prevent you from seeing a malicious file.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

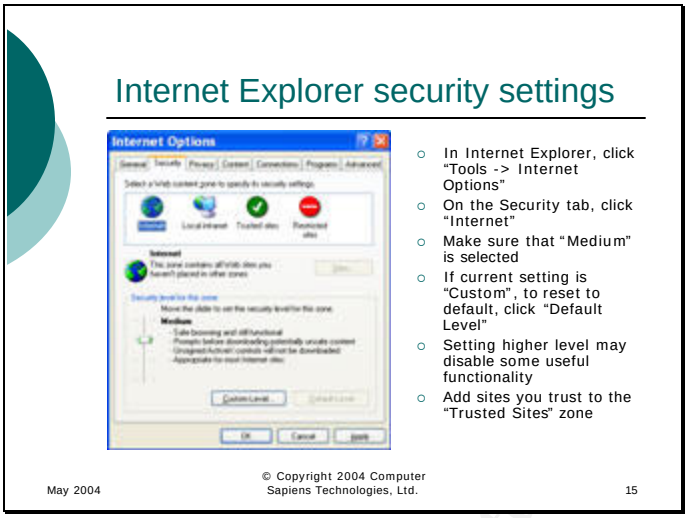


In each Microsoft Office application you have installed, make sure that you configure macro security to at least Medium level. To open the macro security dialog, click “Tools -> Macro -> Security.

With medium security, when you open a document, you will be notified if it contains macros and you can choose whether or not you want them to run. If you do not expect any macro functionality in the document or a spreadsheet, say “No” to the prompt.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

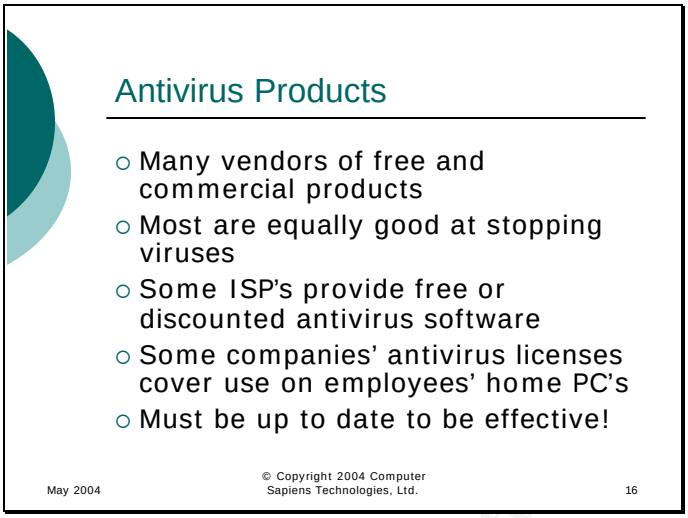


To set a minimum security level for web sites you visit, make sure that the security level for the Internet zone is set to "Medium" or higher. This will stop most unsafe active content and prompt you before installing or downloading anything from the Internet. You will still have the functionality you need while protecting yourself from the most common online, web site booby-traps.

If you notice that one of the sites you used to visit has stopped working after you made the change, you can add it to the "Trusted" zone. Click on "Trusted sites", then click the "Sites" button to add the site to this zone. You may need to clear the checkbox that says "Require server verification (https:) for all sites in this zone".

Of course, in order to be even more protected against online hazards, you can set the security level for the Internet zone to "High", or to "Custom" and then disable all active content. However, this will break the functionality of mostweb sites as they rely on active content to give you an interactive, personalized experience. As always, this is a trade-off between usability and security. If you want to be totally secure, keep your computer turned off.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



One of the key components of your protection against malware is a good antivirus program installed on your computer. There are many, and although each one claims to be the best, they are all quite good at detecting most malware, provided you keep whichever one you have up to date.

There are a number of commercial products on the market such as McAfee, Symantec (Norton), and many others. The cost is usually quite reasonable, and they come with technical support which may be worth the cost of the product to you. However, there are also a number of free antivirus products that may have fewer configuration options but are still equally good at protecting the average home PC from most infectors. One of the free products I quite like is AVG Antivirus (http://www.grisoft.com/us/us_dwnl_free.php).

There are also free online antivirus scanners. The problem with those is that you can come and scan your PC for infections, but they do not provide continuous protection against viruses and other malware. Because of this, you should only use them as a "second opinion" to verify that your regular antivirus program has not missed something. On the other hand, you can count on the online engines to be always up-to-date with all the latest definitions.

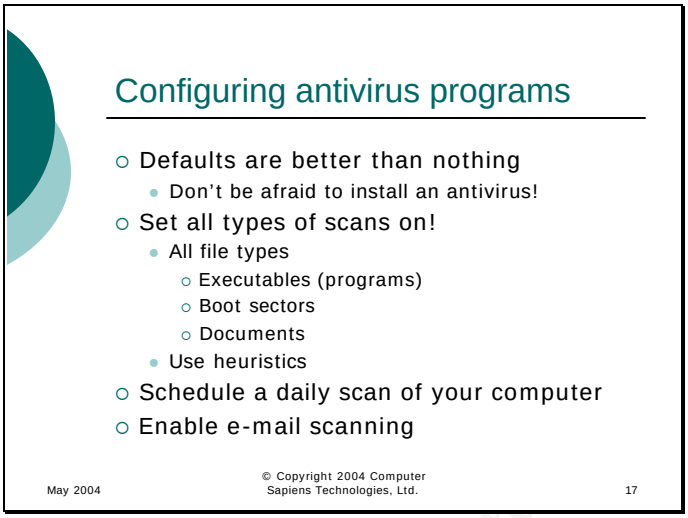
In addition, many ISPs (Internet Service Providers) give you a copy of an antivirus program just for becoming their customer. One of the examples is Telus in Canada - it gives a copy of an antivirus program and pop-up blocker with its high-speed service, and also provides a spam filter for free.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

No matter which program you use and where you got it from (computer store, free download, from your ISP), it absolutely must be very up-to-date for it to be effective. What good is the program that can only detect the viruses that existed last month and is unaware of the ones that are spreading like brushfire today?

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



When you install an antivirus, some of the settings are pre-configured right out of the box. Most scanners will try to strike a compromise between protection and speed by only scanning some of the file types, or only scanning for known viruses instead of using heuristics. Although this is much better than nothing, most computers today can easily handle the load of increased scanning without too much impact on speed. So, although you should install an antivirus program even if you do not change any of the settings, you should look at additional options you can enable in the program in order to get additional protection.

First, enable scanning of all file types. It is no longer safe to assume that just because a file seems to be of a "safe" type (music or picture), it cannot carry a virus. There are exploits that use vulnerabilities in how such "safe" files are handled by the operating system to make your computer execute some malicious code.

Second, enable heuristics unless you have a very old, slow computer. If you do have such an old machine, using heuristics may slow it down too much – that is your hint that perhaps it is time to upgrade.

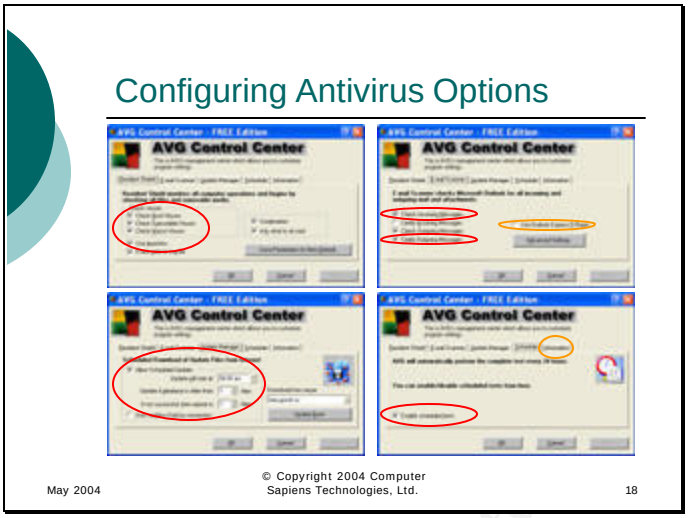
Schedule a daily full scan of your computer. Try to run it some time when the computer is on but you are not using it. Some people tend to turn off their computers at night – perhaps you should consider leaving it on some days and schedule a scan every night. That way, when you want to run a scan, just leave the computer on when you go to bed. If you shut the computer down, the scan will obviously not run that night.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Always enable e-mail scanning. This way, if an infected attachment is detected, it will be deleted or replaced with a text file with details of the infection before it gets a chance to infect your computer.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

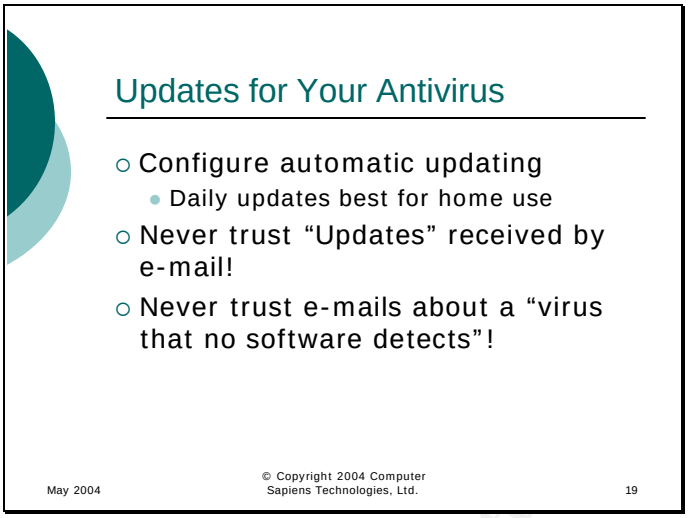


These are screen shots of a well-configured copy of AVG Antivirus. Notice that all file types are scanned, heuristics are enabled, all messages are checked and outgoing messages are certified as virus-free after being checked by the antivirus. Since the computer these screen shots are from is not using Outlook Express, Outlook Express plug-in is disabled; if you do use Outlook Express, you should enable this checkbox.

On the bottom left, you see the update scheduling. Notice that the program is configured to check for updates every night.

On the bottom right, you see that scheduled scans are enable. The free version of AVG does not allow you to specify the time f the scan and it happens at 11PM. I always leave my PC on at night, so it is scanned every night. On the same screen shot, you see an orange circle around the Information tab – if you click that tab, you can see the version of the software and, more importantly, when the virus definitions were last updated. If they are older than a week or so, you may have a problem and may need to update them manually by clicking the “Update Now” button on the Update Manager tab (and, of course, figure out why they are not happening automatically).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



The easiest way to keep your antivirus up to date with the latest virus definitions is to configure automatic updates. Many companies configure updates to happen many times a day, so that new definitions are installed as soon as they are available (every available update means there is a new virus out there!). However, for home use, it is enough to have an update scheduled once a day. In the future, it is likely that you will need to configure multiple updates per day since viruses are spreading faster and faster.

Never trust an "update" received in an e-mail. Antivirus companies do not send out updates in e-mails. Even if you get an e-mail with a link to an "update", it is likely to be a fake, and clicking on the link very well may get you infected with the latest virus. To update your software, always use the antivirus program's interface since it is configured to go to the correct server.

Another thing you should never trust is an e-mail telling you about a "virus" that no antivirus software detects. Usually these e-mails will instruct you to find and delete some file on your computer. Never follow those instructions or trust these e-mails, no matter how scary the "virus" sounds or how convincing the e-mail seems. These e-mails are always hoaxes and following the instructions in them will only lead you to deleting a useful (or critical!) part of your operating system. Think about it logically: if whoever sent you the e-mail knows about the virus, surely so do the professionals at the antivirus company. And if getting rid of the virus is as easy as deleting a file, surely it is not hard

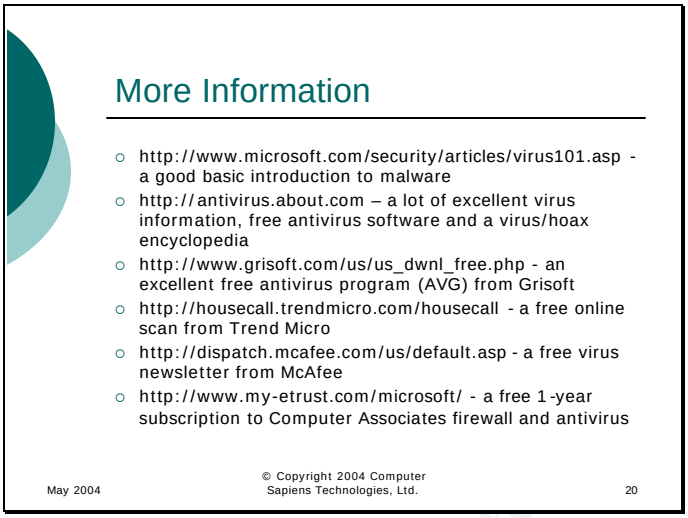
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to release an update to the antivirus program to do that. Besides, how does whoever wrote the e-mail know that the file is a virus if no antivirus program can identify it?

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

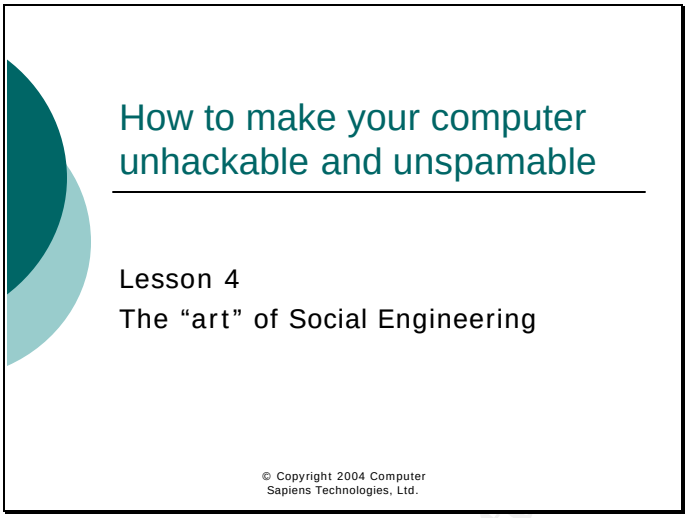


There is so much malware-related information on the web that it is easy to get overwhelmed. However, most sources will tell you the same thing, so it is enough to find one or two that you trust and stick with them. Above is a good selection of starting points.

I would strongly recommend subscribing to a virus newsletter from a reputable company such as Sophos or McAfee. In addition, you can see a link to AVG antivirus software and a free online scan from Trend Micro. It is a good idea to run an antivirus program from one vendor on your computer and use a different vendor for occasional online scans.

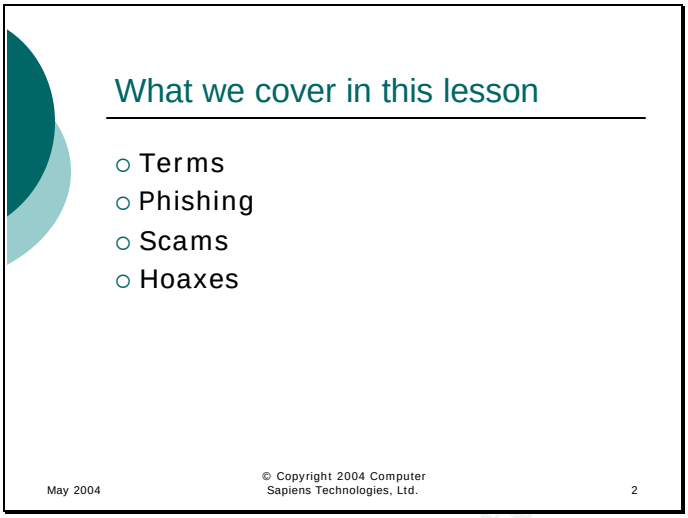
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

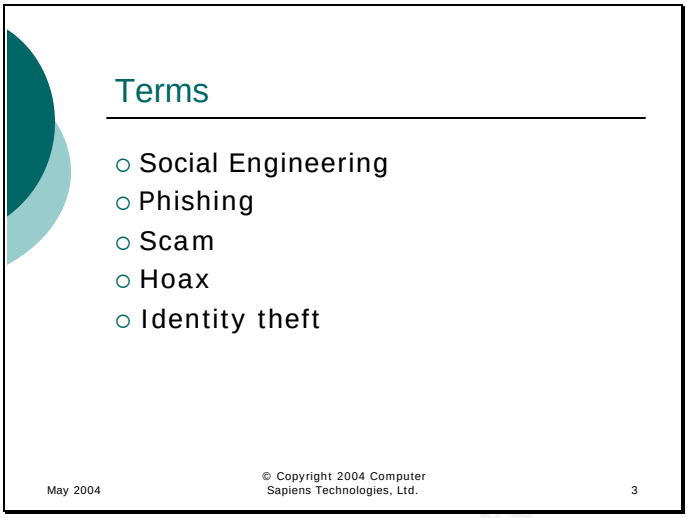


In this lesson, we will discuss the part of security that is often overlooked – the “human element”. We can build many walls around our castles, but if the guard at the drawbridge is easily convinced to lower it to someone with a smooth look and a good story, all the bastions in the world will not help.

As always, we will start with some of the terms used to discuss these matters. Then, we will talk about three main types of attacks that use a convincing story to trick you into doing what the attacker wants: phishing, other scams, and hoaxes. We will talk about how to recognize such an attack, where to confirm whether a story you are being given is legitimate or not, and how to deal with scams.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



First, a few terms.

Social Engineering - euphemism for cons. It covers anything that is done by convincing an operator or user of a system to do what the attacker wants without using technical methods to break the defenses.

Phishing – using a false story to get a user to send their financial or privileged personal information to an attacker.

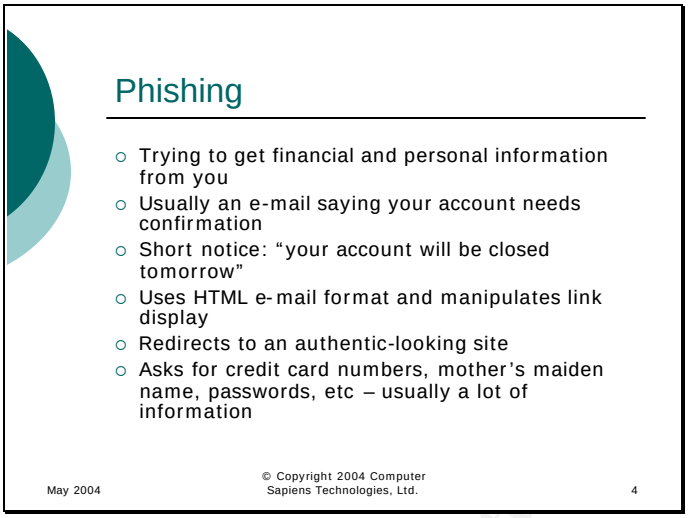
Scam – just like the old-time phone scams, this term covers a broad range of activities where a false pretext is used to get at your money.

Hoax – a false story, usually designed to cause harm but generally does not attempt to get any information back. A false rumour.

Identity Theft – obtaining enough information about you to use your name to obtain credit or perform other activities under your name, leaving you to deal with the mess.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

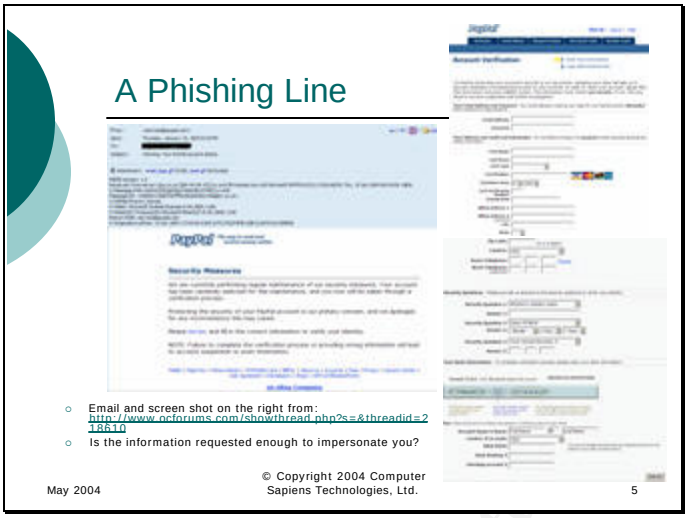


Webopedia (www.webopedia.com) defines phishing as:
Phishing (v.) Pronounced "fishing," the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

As a rule, the e-mail says that your account needs to be confirmed and looks very legitimate. The recent phishing scams use a number of tricks– they use graphics and icons from the real site of the company they are supposed to have come from, and they manipulate the hyperlink display in order to give the impression that they point to the real site. If you click on the link, you get directed to an authentic-looking site that asks you for a lot of personal information – credit card numbers, banking information and a lot of other data which is often used to confirm your identity – your mother's maiden name, Social Insurance or Social Security number, passwords, etc. – the information that is later used to impersonate you for financial gain.

A common tendency among these e-mails is short notice – the con artists do not want you to have enough time to confirm the facts or contact the company the e-mail supposedly cam from, so they often say that action is required right away.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



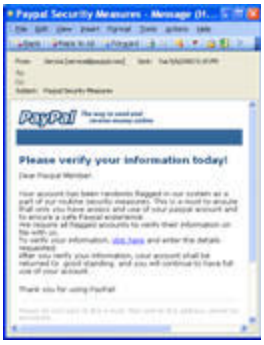
This is an example of a phishing scam e-mail and the site the link in it takes you to. As you can see, there is a PayPal logo and the site uses a menu bar at the top that looks like the real thing and even takes you to the real site to avoid suspicion.

Look at the information requested on the right: login and password (enough to impersonate you on PayPal), credit card including the verification number and billing address (enough to use it for online purchases), home and work phone (can be used to fake a call from you by manipulating Caller ID functionality), security questions that most financial institutions would use to confirm your identity, and banking information sufficient to transfer money out of your account, especially combined with the information above.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Another phishing line



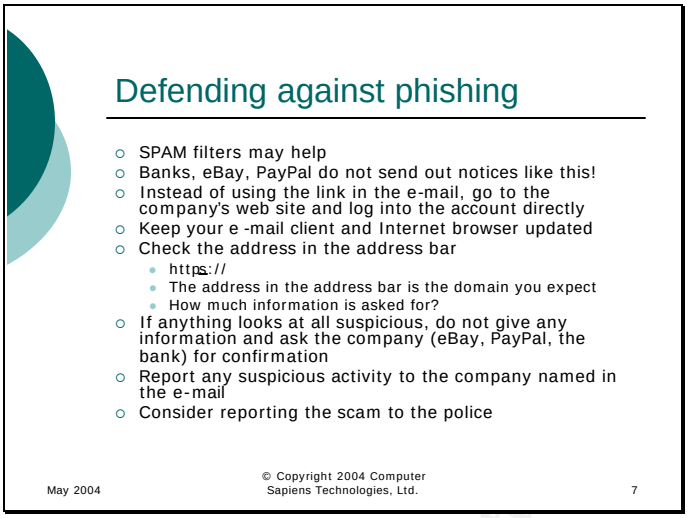
- Email on the left arrived in my own mailbox
- Texas man pleads guilty to phishing scam (Reuters): http://www.usatoday.com/tech/news/internetprivacy/2004-03-22-done-phishing_x.htm?POE=TECISVA
- E-Mail Scammer Gets Four Years (Reuters): http://www.securityfocus.com/news/8711

© Copyright 2004 Computer Sapiens Technologies, Ltd.

Here you see a phishing e-mail that arrived in my own mailbox a little while ago. The idea is the same, the story is slightly different.

Governments all over the world are now beginning to take phishing and other online scams seriously. For example, a man was arrested in Texas and sentenced to four years in jail for sending millions of fake PayPal e-mails like this one. However, the overall number of phishing scams did not decrease noticeably with his arrest.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



The best defense against phishing is not to trust every e-mail that arrives in your mailbox purporting to be from your bank or another online financial institution. Spam filters may help – since phishing e-mails are tagged by spam filters as spam (and they are), most will be filtered out. However, when a new one surfaces, you may still get it before the spam filter is updated to recognize the new variant.

Banks and financial institutions will not send e-mails with links for account verification, so if you get one, it is almost certain to be a fraud. If you suspect that the e-mail is fraudulent, do not click on the link in it. Instead, open your web browser and go to the company's web site. Log into your account and verify that there are no problems. All of the companies that do business online have a way to contact them on their web site – send them an e-mail with the details of the notice you received and have them verify whether it was legitimate (probably not).

Some of these messages and sites exploit vulnerabilities in your e-mail client or web browser, so keep them up to date. When you are at an online banking or financial site or are giving your financial information to any entity on the Internet that you trust, make sure that the site is authentic and not spoofed:
The page address should start with "https://" and not "http://"
The address of the page is what you expect
The page is not asking for unusually large amount of information

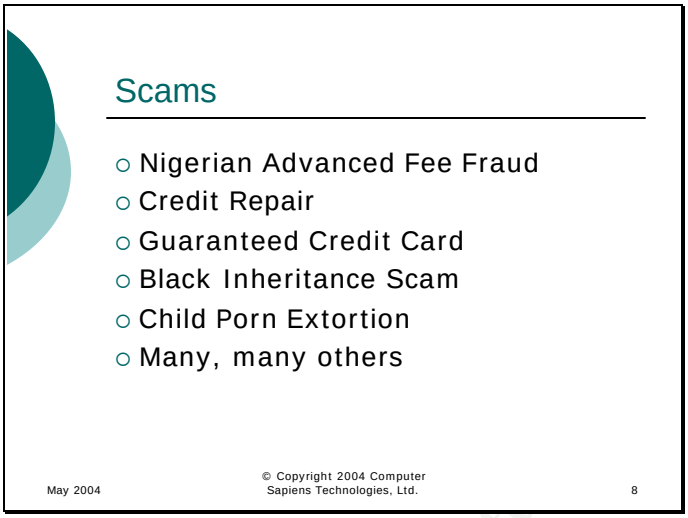
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

If anything looks suspicious, do not fill out any form and contact the company for confirmation. If you get a suspicious e-mail, report it to the security department of the company it supposedly came from. For PayPal (most phishing e-mails fake that service), the address of the security center is: http://www.paypal.com/cgi-bin/webscr?cmd=_security-center-outside

If you believe that the fake is very good and may cause real damage, do not hesitate to report it to your local police (use the non-emergency number). Police departments now pay more attention to online crime and you should be able to talk to someone who deals with online scams. They should take your report, and if they are not aware of the specific e-mail you have received, they will tell you how to send them the message in such a way that they can investigate its origin and potentially notify a federal or international law enforcement agency.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



There are many schemes that exist for extracting money from people.

One well-known scam is the Nigerian money transfer scam where you get an e-mail asking you to help transfer money out of Nigeria in exchange for a large reward when the funds are transferred. The stories vary but the victim is either asked to provide the details of their bank account, or (more often) some money for "transfer fees" or "taxes" or other expenses, and the windfall never arrives, of course. People have lost tens of thousands (I have read reports of up to $5 million) hoping for a huge payoff in the end.

A Credit Repair scam and a somewhat similar Guaranteed Credit Card scam prey on people with poor credit histories. "Credit Repair Specialists" charge a fee for instructions on how to repair your credit history – and that is, according to the governments, quite impossible using legal means, other than through time and being responsible with your credit obligations. In a number of cases, the instructions contained suggestions on using a different Social Security Number for applying for credit – and that is a felony.

The Guaranteed Credit Card scam offers a major credit card regardless of your credit history. The company always charges you a fee up front ($100-$200) but you are not likely to get the major credit card from them. Instead, you will probably get the company's own credit card that can only be used to purchase items from their own catalogue of items – and once you purchase the required number of items, they will send you a general VISA application for a legitimate bank and a nice letter telling you that by using their card, you improved your credit card and may now qualify for a VISA

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

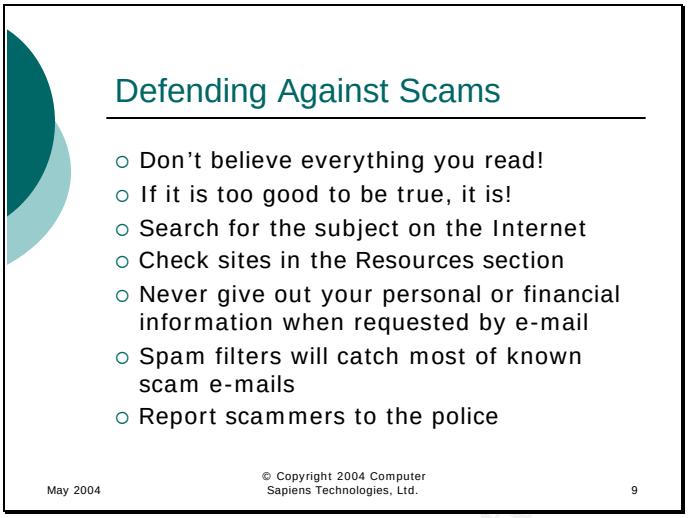
(if your prior credit history was bad enough to use such desperate measures, you still don't).

The Black Inheritance Scam tells you about the Federal Tax Refund you may qualify for if your ancestors were slaves and charge you $100 to help you with the paperwork. There is no such refund.

The Child Porn scam is fairly new. You receive an e-mail saying that child pornography has been planted on your computer by hackers and for a small fee ($20-$30) they will not report you to the police. There is no child porn on your computer, of course, but a lot of people consider the sum small enough to be "better safe than sorry" and pay up. This is extortion and a variation on an older scheme where companies were charged tens of thousands for not having their servers shut down by hackers.

Of course, there are many more scams. Unlike the telemarketing scams of a few years ago, they can now be created faster and it does not take long to send an e-mail to millions of people. Your best defense is common sense – if an e-mail offers something for nothing, it is likely to be a scam. If it offers something that should not be possible, it is probably a scam.

© SANS Institute 2004, Author retains full rights.



Defense against online scams is really no different than defense against scams of any other kind. After all, the scams are substantially the same – they are only using a different medium to reach you.

First, do not believe everything you see or hear or read – that stands true, no matter what medium is being used. Even if the sender of an e-mail is someone you know, they may have been scammed themselves into forwarding a copy of the fraudulent e-mail to you.

If an offer sounds too god to be true, it more than likely is! If someone is telling you that you can get a lot of money for nothing, you are being taken.

One of the quickest ways to check whether the "offer" is a scam is to do a search for the subject of the e-mail using your favourite search engine like Google or check your favourite security or antivirus site – most have an extensive database of current scams and hoaxes. Check with the Better Business Bureau – they often have data on fraudulent operations. The Resources section of this lesson has a few links to good places to start checking out a possible scam.

Never give out personal or financial information to someone who contacted you. That is a good rule of thumb in all methods of communication. Never trust a phone number or a link that was given to you, only ones you found independently. Basically, if you called your bank's number, you are likely talking to the bank; if someone from the bank called

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

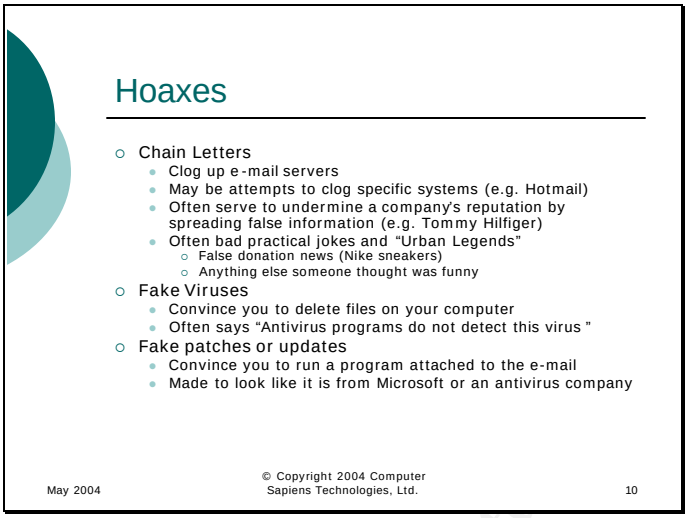
you, you have no proof who they actually are and should not give out any information. The same principle should apply to your online behaviour.

Use a spam filter – they generally catch most of the known scams as they use unsolicited e-mail (spam) to reach potential victims.

If you see a scam that is easy to believe (especially ones that almost got you – or did get you tho believe that they were “for real”) – call the police. Call the non-emergency number and ask for the computer crimes division. Slowly but surely, most police forces are beginning to take online crime seriously.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Hoaxes are e-mails or rumours that do not have a goal of taking any of your money. At best, they are practical jokes on a large scale; at worst, they intend to damage someone's reputation or try to convince you to delete important files on your system. A virus that propagates by pretending to be an update from a software manufacturer can be considered a hoax or a blend of a virus carried by a hoax e-mail.

Many hoaxes take the form of chain letters. There are many false rumours that are still propagating among the Internet users about Nike collecting old sneakers or a sick kid in England who needs postcards to get better. All chain letters end with a request to forward them to as many people as you can.

Chain letters are often designed to clog mail servers, or to cause some harm to a company. An example is the false rumour about Tommy Hilfiger making racist statements on TV. Some chain letters are relatively harmless practical jokes (Nike collecting old footwear hoax) but they can waste your time and the time of anyone you send them to.

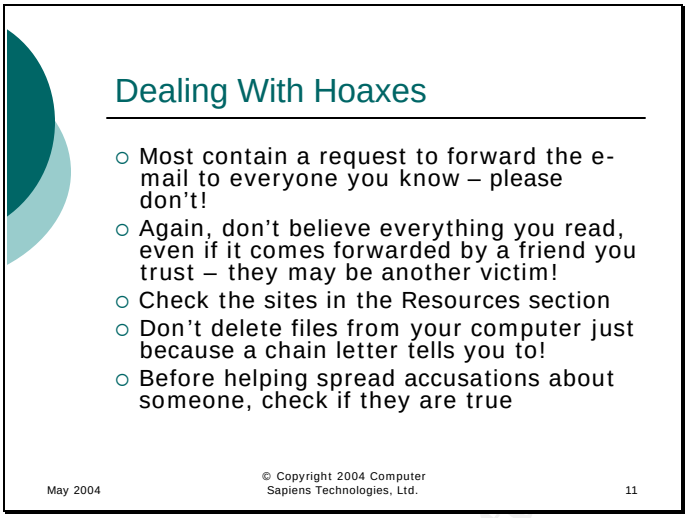
Fake virus notices generally start with a description of a terrible virus tat will cause great damage to your system but is somehow not detected by any antivirus software. You are instructed to check your computer for a specific file and delete it if you find it. The file is one of the parts of the operating system, so it will be on your computer and by deleting it, you are removing some of your system's functionality.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Occasionally, a hoax (a vulnerability has been detected – you need to apply this patch right away) carries an actual virus as an attachment. These e-mails often look like they came from the manufacturer of a piece of software that most users have (like Windows).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Rule #1 (I found it to be 100% accurate): Anything that asks you to forward it to people is a hoax. Although it is possible that there may be exceptions to this rule, I have not encountered any. Do not blast a copy of an e-mail to everyone in your address book just because it asks you to!

Rule #2: No matter who forwards you a chain letter, do not assume that they checked it out and verified it as being true. The chances are that they did not know Rule #1.

Rule #3: Keep your antivirus up to date and trust it. If detecting a virus is as easy as searching for a specific file and getting rid of it is as easy as deleting a that file, don't you think that antivirus companies could figure out how to include that into their definitions faster than it would take a chain letter to reach a significant number of people? Also, the person who sent the first copy of that letter – if no antivirus software detects the virus, how did he know that that file was one?

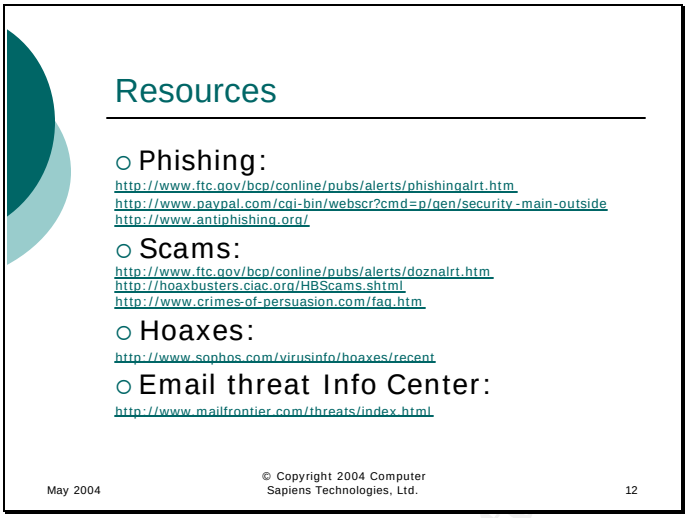
If an e-mail arrives asking you to boycott a certain brand and telling you awful stories about the company, always verify the information before joining the boycott or resending the letter! The chances are that the accusations are false – hoaxes exploit our trusting nature and laziness: sounds plausible, and who has the time to check? Spreading false rumours about someone is a crime – don't become someone's accomplice!

Again, refer to the sites listed in the Resources slide to do research on hoaxes and do a quick "Is this a hoax?" check when you get a chain e-mail.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



These are just a few of the sites that offer scam and hoax information. It does not take long to check, and a check can save a lot of grief for someone, often yourself. After I Verify that a chain e-mail is a hoax, I generally send a reply to whoever sent it to me with a link to the information I found. I found that slowly but surely, people who used to send me those e-mails with the best of intentions, stop doing it. I have no proof that they do not resend them to anyone else – but at least, they no longer send them to me. Good enough.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

How to make your computer unhackable and unSPAMable

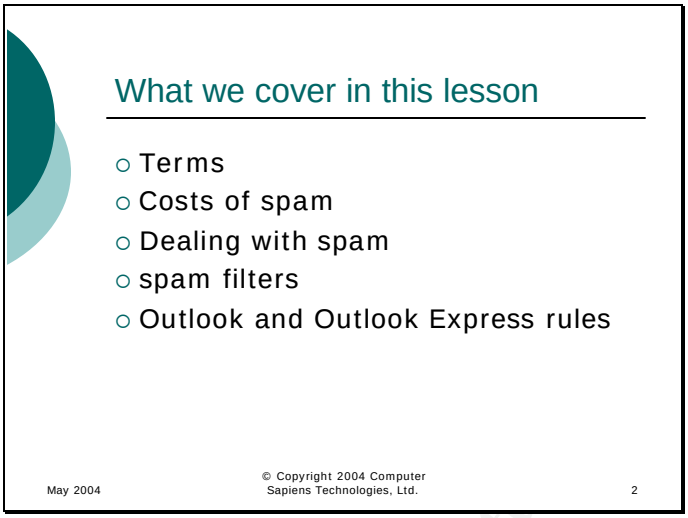
Lesson 5

spam, spam, spam

© Copyright 2004 Computer Sapiens Technologies, Ltd.

© SANS Institute 2004, Author retains full

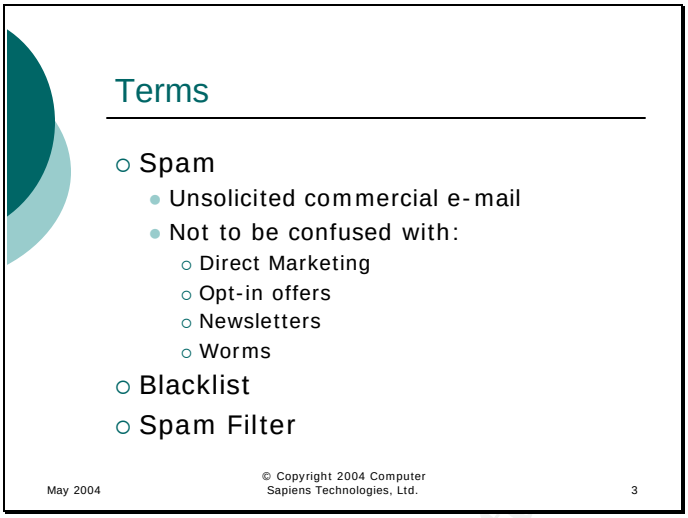
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



This lesson deals with spam, or unsolicited commercial e-mail. We will talk about why spam is considered a major problem, how to deal with it, and some of the tools at our disposal that can help us minimize its impact on our lives.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



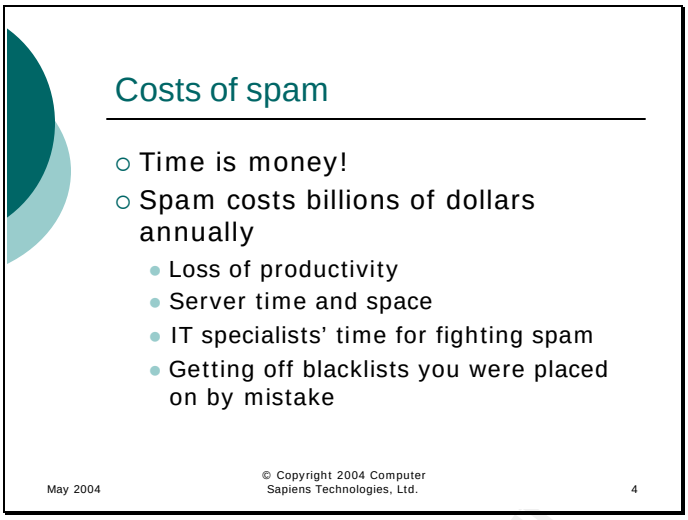
Spam is unsolicited e-mail offering products or services and usually indiscriminately sent to a large number of people who do not want it. It is a blatant abuse of the e-mail system and is illegal in many countries.

It is often confused with:
Direct marketing – for example, offers of new products or services sent to existing customers of a company
Opt-in offers – when you sign up for a service, you may be asked whether you would like to receive offers from other companies
Newsletters – some newsletter writers can be quite prolific and send dozens of updates per day. Although many newsletters are supported by advertising, they are not spam as long as you subscribed to the newsletter.
Worms – although they are unsolicited and may arrive in your mailbox, they are not advertising anything.

Blacklist – a list of servers that have been known to send out or relay spam. Such lists are maintained by a number of companies and others can rely on those list to block e-mail from any server on that list.
Spam Filter – a program that runs either on a mail server or your computer that tries to detect spam messages

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



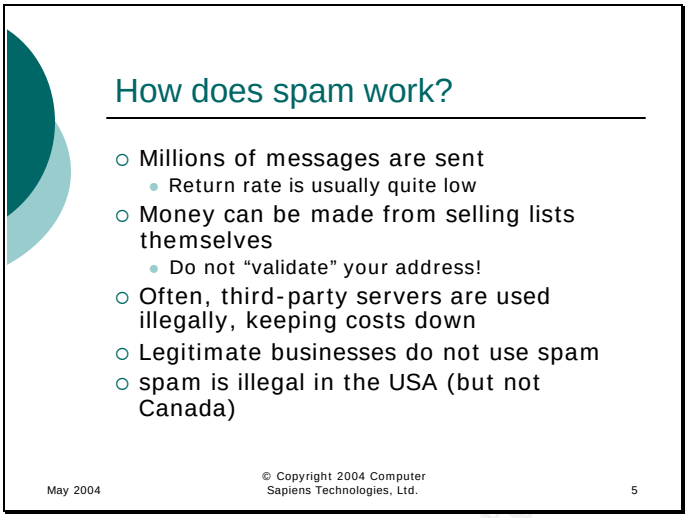
The cost of spam is huge. However, very little of it is the cost to the spammer – and most or all of the cost is carried by companies, ISPs (Internet Service Providers), and end users:

Since even deleting a spam message without reading it takes time and interrupts your thought process, this impacts your productivity at work – if you get spam there.
At home, you have better things to do than be inundated with offers of products you do not want.
ISPs and corporations need to buy more powerful mail servers so that they are not overloaded with spam and legitimate mail can still get through.
Spam filtering software is rarely free – and needs to be purchased to minimize spam that gets through.
Specialists that maintain mail servers are not cheap, and a large portion of their time is spent dealing with spam.
Networks and network equipment need to have higher throughput in order to not be swamped with spam.
If someone makes a mistake and puts your server on a blacklist, it takes a long time to get off – and in the meantime, your users cannot send legitimate e-mails to their contacts. Sales are lost, productivity goes down.

There are other ways that spam affects us all – but most of it wastes people's time – and as we know, time is money!

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Spam works by playing odds. Although the percentage of people who respond to offers in spam is very low, it is not zero. So, by sending a very large number of messages, the spammer increases the number of people who respond, even though the vast majority does not. Since sending a million messages costs nothing or very little to the spammer and they may get one sale in return, it makes spam worthwhile to the spammer.

A "validated" list can also be sold to other spammers. An e-mail address is considered valid if there is proof that it actually belongs to someone. That is why many spam messages will request read or deleted or delivered receipts – the receipts can be gathered and the list of addresses that the receipts came from would be considered a validated list. When you click on a link in a spam e-mail to "check out" the product, your e-mail is validated – and you will get more spam, even if you do not buy anything. There are other tricks spammers can use – for example, embedding an image link into the e-mail. When you open or even preview the message, the link is used to display the image – and the request for the image will generally send your e-mail address to the spammer's server, validating it – so you can validate your address just by looking at the spam message.

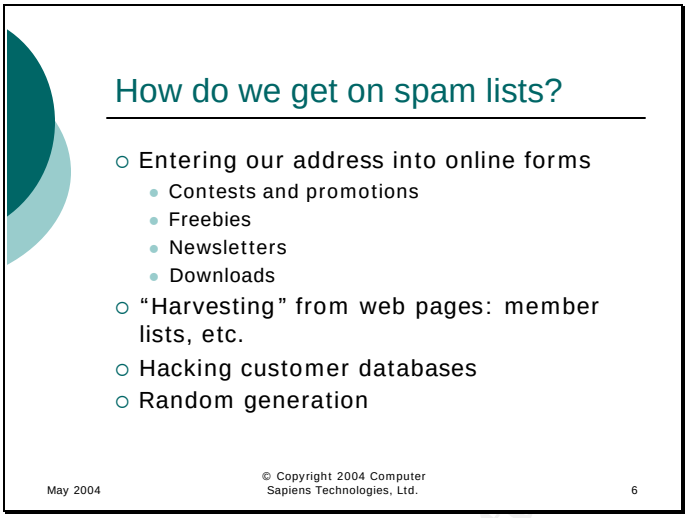
To keep the costs down and to avoid detection, spammers will rarely use their own e-mail servers or those of the ISP providing them with Internet access. Rather, they will search for unprotected server belonging to unsuspecting people or companies and use those servers to send out their advertisements.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

At this point, most of the spam you see is selling porn or pharmaceuticals or natural supplements of dubious origin, as well as counterfeit software and some other “shady” products since legitimate businesses have realized that this method of advertising does not pay. Although in the past, there was a good chance that an offer that arrives in an unsolicited e-mail was legitimate, by now it has got to the point where it is very unlikely to be. A legitimate business would be too afraid to ruin its reputation by being associated with spam, so it will rather buy advertising space in newsletters or use other methods (promotions, contests) to get word of their products to new customers. So, it is safe to assume that spam has no real value to the economy as a method of advertising legitimate products or services.

Because of that, outlawing spam has no negative effect on legitimate economy and some countries have made it illegal because of the heavy burden it places on everyone. However, spammers are generally quite good at avoiding detection and finding and prosecuting them is still difficult. In addition, there are a lot of countries that have not passed anti-spam laws, and a spammer can simply move their operations there if necessary.

© SANS Institute 2004, Author retains full rights.



Time after time, people ask: "How did those people get my e-mail address?" There are many ways that your e-mail address could have ended up on a list that then got resold to others.

Have you ever entered a contest and gave your e-mail address to be contacted in case you win a prize? Did you read the rules of the contents? Do you trust that the company that runs the promotion will not disclose your e-mail to others? Some companies are more serious about your privacy than others, but in the end, all companies run those contests to make money somehow. As a rule, contests are run in order to gather customer data and it is up to you to check how they intend to use that data and to decide whether you trust that company enough to give them your e-mail address.

The same goes for freebie offers. Most of the time, a company offering a free sample of a product is simply looking to interest you in buying it later, but occasionally freebies are advertised by less scrupulous people to gather e-mail addresses for a spam list.

Most newsletters do not sell their address lists because they would rather sell advertising space in their issues than lose their subscribers by selling the entire address list. However, it is possible that by giving your e-mail address to a newsletter author you are taking the first step to ending up on a spammer's list.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

When you download free software, you are often required to register at the author's site. The registration information goes somewhere – and sometimes, it may end up on a spammer's list.

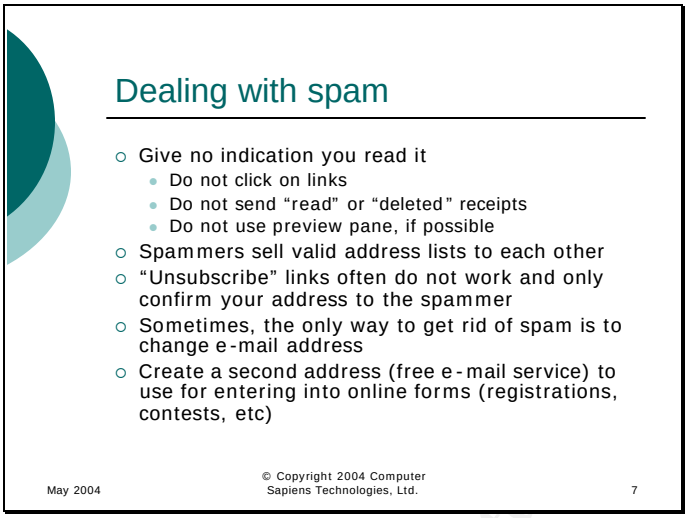
However, from a spammer's point of view, buying customer lists is a slow and expensive process. Most newsletters only have a few thousand subscribers, while a spammer generally sends out millions of e-mails to get enough responses to make it worth their while. So, spammers will often take more aggressive approaches:

There are tools that will search the web for e-mail addresses embedded into web pages. For example, if you have a family album on the Internet with public access to it and your e-mail address on one of the pages, it is virtually certain that sooner or later, that address will be used to send you spam. Also, many community organizations list e-mail addresses of their members or officers on their web pages – they will be harvested. Online forums need to be careful not to list members' addresses directly (there are techniques to hide them).

A hacker can also attack a company's site and gain access to the customer database, extract customers' email addresses and sell the list to spammers.

Often, spammers resort to randomly generating e-mail addresses to try and come up with ones that work. For example, most companies have at least one person named John. So, an e-mail to john@company_a.com or john@company_b.com is likely to succeed. By combining a list of common names with a list of corporate and ISP domains, anyone can come up with a huge list that will have some valid addresses in it – without going through the trouble of actually buying or harvesting real address lists. Although most e-mails sent to a list like that will fail, some will get through – and that may be enough for the spammer.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



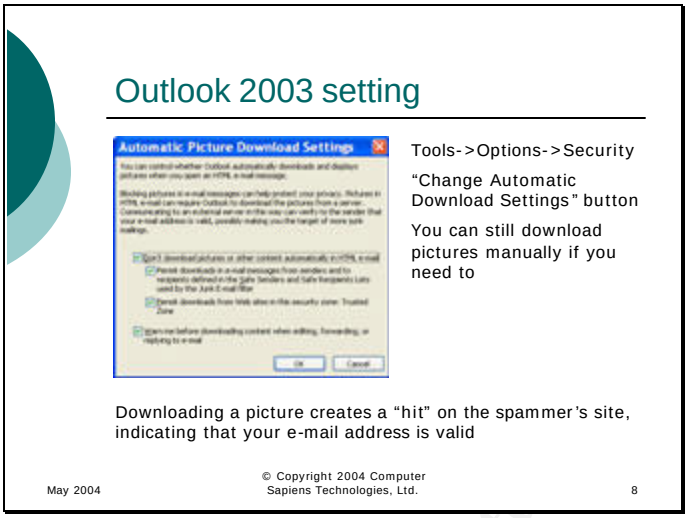
When dealing with spam, there are two main strategies you can use to reduce the amount of spam you get (to get rid of the spam that comes through anyway, use the filtering techniques discussed later).

The first technique involves pretending that you do not exist. When you receive a piece of spam, do not acknowledge it in any way – do not open or even preview it, do not allow your computer to send read receipts automatically, never click on any links in the e-mail. Any confirmation that you received the message will lead to your e-mail address to be considered "confirmed" and included in a list that will be sold to other spammers.

"Unsubscribe" links in spam rarely work and generally only serve as a confirmation that the address is valid. Do not try to use them to get rid of spam – you will likely only get more.

The second technique involves being able to change your e-mail address as soon as it becomes too well known to spammers. To do that, you need to keep two e-mail addresses: one private, known only to your family and close friends; the other one (a free online service like Hotmail) to be used for entering into contests, etc. When the second address starts attracting too much spam, it can always be changed without too much trouble.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

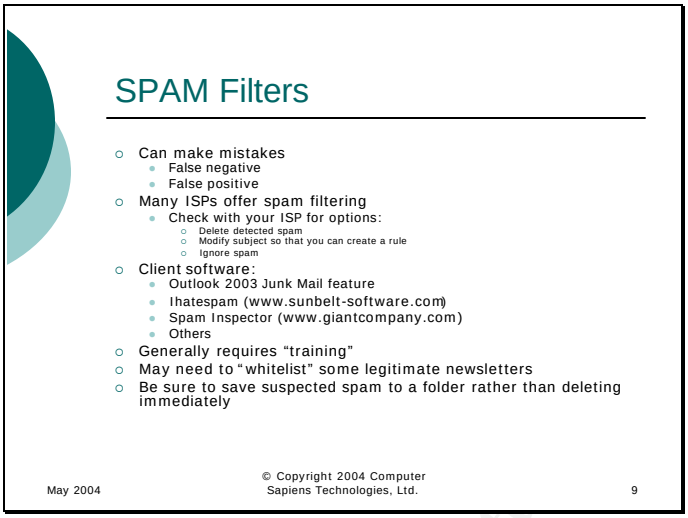


With Outlook 2003, Microsoft introduced a useful new feature for minimizing the amount of spam you get every day. As you recall, many of the pictures embedded in e-mails are actually downloaded when you view the message, rather than being part of the message itself. When you view the message, your computer downloads the picture from the sender, validating your e-mail address and therefore likely causing more spam to be sent. Outlook 2003 allows you to disable this behaviour and nod download all the pictures automatically.

If you enable this feature, you can still download all the pictures in an e-mail manually if you trust the sender and need to see them.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



If you prefer not to have to change your e-mail address occasionally, you have to rely on spam filters to automatically separate spam from legitimate e-mail.

A spam filter is a program that checks each e-mail and decides whether it is spam or not based on a number of factors, such as the sender, the subject, the recipient list (was it sent directly to you?), etc. All spam filters make mistakes from time to time and should be checked periodically. The mistakes fall into two categories: false positives (legitimate mail treated as spam) and false negative (spam getting through the filter undetected). Given the choice, I would rather have to deal with a few spam messages slipping by than having to check my spam folder every day for messages that were falsely tagged as junk – so I try to configure the filters so that I get no false positives at the expense of seeing a few false negatives.

The easiest way to filter out spam is to enable the filtering that many ISPs provide, either free or for a nominal fee. This gives you the benefit of always up-to-date, server-based filtering. The downside is that if the server filter does make a mistake, you cannot configure it to allow (or block) specific senders or subjects directly. However, in my experience, an ISP filter tends to be more accurate and less of a hassle to configure than a filtering program installed on your own computer.

When you configure an ISP spam filter, you will generally get three options: No filtering, Delete immediately, and Tag as spam. Especially in the beginning, you want to use the Tag option that modifies the subject of suspected spam mail by adding a recognizable

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

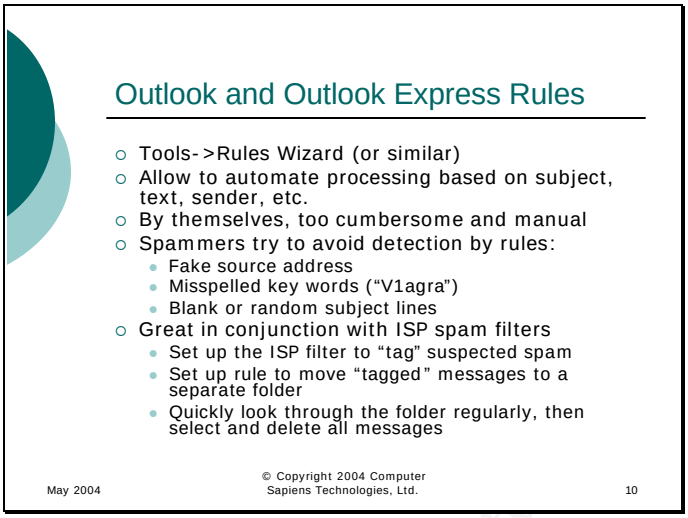
“tag” to it. You can then configure a rule in your e-mail program (Outlook or Outlook Express) to move tagged e-mail to a special folder. If you do not know how to use such rules, the ISP’s web site or the e-mail program’s Help should be able to guide you.

If you prefer to have more control over the messages that are filtered out, you will need to get your own spam filter. You can use the one included with Outlook 2003 e-mail client, or you can purchase a third-party application such as IHateSpam (there are also many others). No matter which application you choose, you will need to train it to recognize spam and allow legitimate e-mail through.

Especially for the first while, make sure that you do not configure the filter to delete the spam automatically – instead, configure it to move spam to a separate folder. This way, you will be able to check the messages the software considers spam and possibly rescue and “whitelist” some legitimate newsletters or offers you have subscribed to.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

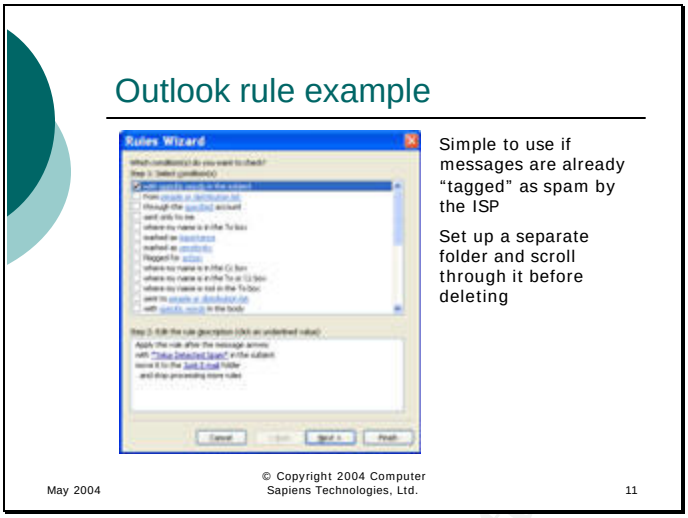


If you are not using Outlook 2003 and do not feel like buying spam filtering software, you can still get rid of the most annoying messages automatically. All you have to do is configure Outlook or Outlook Express rules to check the subject or the body of all messages and delete them if they contain some of the more common terms that appear in spam. Be sure to include most of the spellings of those words – spammers can be quite creative about trying to avoid such rules.

Because of the myriad of ways you can "spell" the same word – Viagra, V1agra, Vlagra, etc. – using rules by themselves gets cumbersome very quickly. Trying to use the sender's address is also unlikely to work since the addresses are easily faked. Overall, you may be able to catch 10-15% of the spam by using rules alone.

Where these rules shine is in conjunction with an ISP's spam filter. First, you configure the ISP's filter to "tag" spam by adding a special string to the subject (for example, "Cheap Viagra" will become "***Suspected spam*** Cheap Viagra". Then, you create a rule to send all messages with "***Suspected spam***" in the subject to a special folder. You can check that folder before deleting it, to make sure that legitimate mail does not accidentally get tagged as spam, but once you get to trust the ISP's rules, you can change the rule to permanently delete all messages with this tag in the subject.

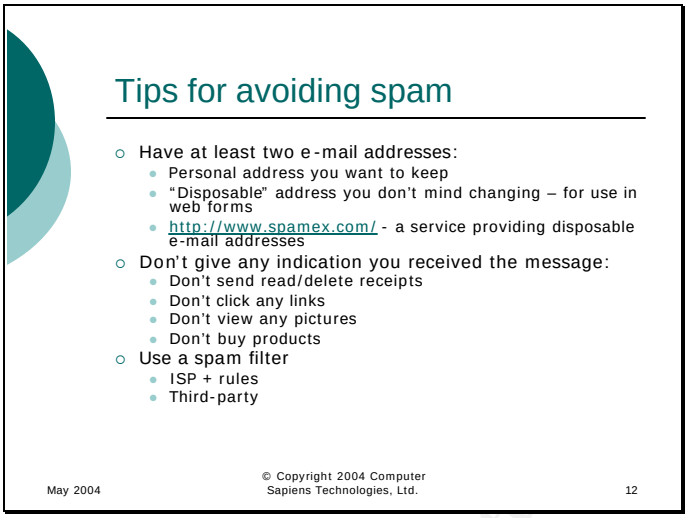
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



This is an example of the Rules Wizard rule – this one is from Outlook 2003. As you can see, it checks the subject of messages and sends them to a special folder if the subject contains the string that is appended by the ISP's spam filter.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Spam is a fact of life these days. Although governments are trying to pass laws that are supposed to decrease the amount of spam we receive every day, the situation is unlikely to change anytime soon. In the meantime, all we can do is try to avoid as much of the spam as possible.

First, you should consider having at least two e-mail addresses. One should be provided to you by your ISP – do not give that address out to anyone but your friends and colleagues. The other one is easy to get from a free e-mail service such as Hotmail. You can use that address for entering online contests, registering products, etc. Eventually, you will notice more and more spam in this second mailbox – then it is time to close that account and open a new one.

There is a service that makes getting a "disposable" e-mail address that is forwarded to your real e-mail address easier - www.spamex.com. For a small yearly fee, you can have them generate as many addresses as you need, even single-use addresses when you suspect that a vendor gives out your address to spammers and want to prove it.

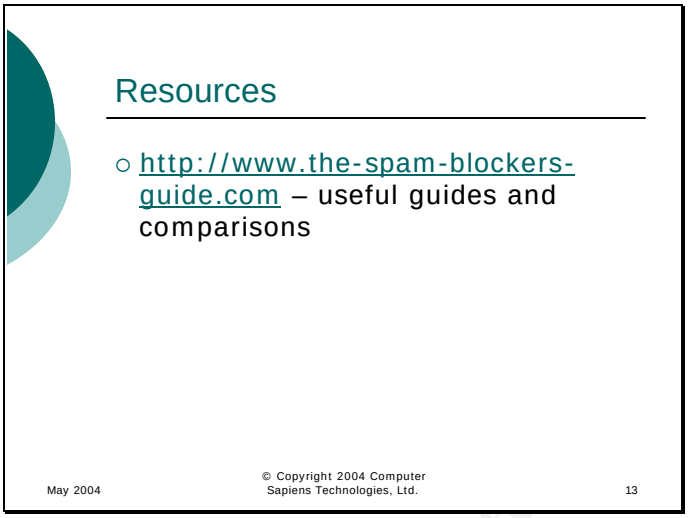
When you do receive spam, the do not give the spammer any indication that you exist and saw the message. Make sure that your e-mail client is not configured to send receipts automatically, never click any links, do not preview the e-mail and most importantly, never "check out" any offer that arrives in a spam message since it not only confirms that you exist, but also tells the spammers that you are gullible.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

To maintain your sanity, use a spam filter, either a third-party application installed on your computer or a combination of a filter from your ISP and Outlook or Outlook Express rules.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



A good resource to check out is the Spam Blockers Guide – it has a few useful guides and anti-spam software comparisons.

© SANS Institute 2004, Author retains full rights.

How to make your computer unhackable and unSPAMable

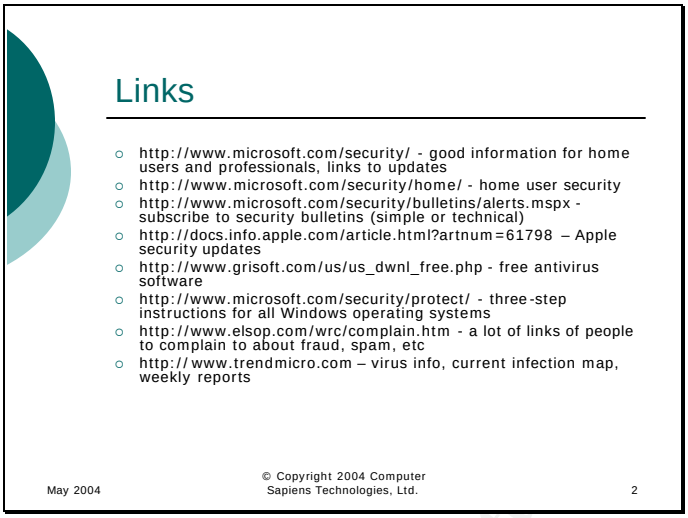
Lesson 6

Where to get more help

© Copyright 2004 Computer Sapiens Technologies, Ltd.

© SANS Institute 2004, Author retains full rights.

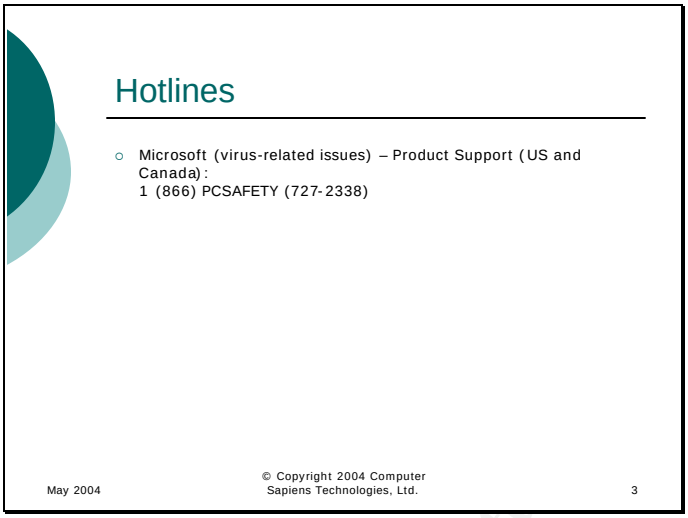
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



There are countless places on the Internet where you can find more information and help when it comes to security. Security companies and professionals are interested in spreading the knowledge to everyone who uses the Internet, so that the average user is more informed and better equipped to keep their computers safe.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Microsoft has established a virus-related hotline for end users. If you have a virus-related issue or questions, you can call them at the number above.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.