Global Information Assurance Certification Paper

Reducing the Catch: Fighting Spear-Phishing in a Large Organization

GIAC (GSNA) Gold Certification

Author: Joel Peter Anderson, joela@umn.edu
Advisor: Richard Carbone

Accepted:
October 9, 2014

Abstract

Email is one of the most valuable tools in the cybercrime kit. To spoof identity, transmit spam or malware, email is certainly one of the most useful methods for communication. In early 2008, universities and colleges noticed a striking increase in campaigns aimed at stealing email accounts, almost exclusively aimed at sending large volumes of spam. The persistent attacks presented a problem for the schools—how to anticipate and prevent such attacks? By using central authentication logging and other network audit tools, the author's university has been working to preempt compromised logins from offshore locations where phishing attacks have originated. This effort is combined with mail system monitoring to stop compromised accounts and reduce the impact of the spear-phishing. This paper examines how audit controls provide a resource that can be used for dealing with new threats.

1. Introduction

The Phishing Problem

> *THE amount of money he annually diverts from wholesome and useful purposes in the United Kingdom, would be a set-off against the Window Tax. He is one of the most shameless frauds and impositions of this time. In his idleness, his mendacity, and the immeasurable harm he does to the deserving—dirtying the stream of true benevolence, and muddling the brains of foolish justices, with inability to distinguish between the base coin of distress, and the true currency we have always among us—he is more worthy of Norfolk Island than three-fourths of the worst characters who are sent there. Under any rational system, he would have been sent there long ago.* *Charles Dickens, 1850*

The phishing problem isn't new. Over 150 years ago, Charles Dickens wrote a passionate and witty letter about fraudsters of his day who, like Nigerian 419 scammers today, preyed upon the generosity and gullibility of well-meaning folk. The differences in our time are that of scale and scope, as the perpetrators have taken on seven league boots and covered continents with their shameless appeals. With automation, every letter is sent not to one or a dozen but thousands of recipients.

These email driven attacks cover a broad spectrum: criminals crafting malware aimed at hijacking bank accounts, others delivering false invoices, preposterous stories of wealth available, or threats of financial (and other) doom are only a fraction of the variety of attacks aimed at Internet users.

On one end, there are the spammers, familiar to everyone with an email account, who present relatively simple advertisements. Forged senders, presenting dubious or illegal wares, send floods of emails that pour into inboxes with their promises of cheap Rolexes or pharmaceuticals.

At the other end of this continuum are the phishers who offer a more intangible "product." Classic is the Nigerian 419 with promises from a "wealthy foreigner who needs help moving millions of dollars from his homeland and promises a hefty percentage of this fortune as a reward for assisting him." The aim of such scams is not immediate payment, but access to personal information, or worse, access to financial accounts.

Author: Joel Peter Anderson, joela@umn.edu

Some phishing scams are much more targeted—"Mission Impossible" scenarios come to life. Cases, like the attacks on the RSA or Google companies, are examples of corporate (and perhaps international) espionage that deliver custom-tailored malware in the guise of an 'innocent' PDF file or spreadsheet forged as sent from a trusted associate, and intended to remove data and credentials from the victim.

Though responsible Internet Service Providers (ISP) and legislation have put measures in place to reduce this flood, users continue to be presented with spam. "Spam has increased from approximately 10% of overall mail volume in 1998, constituting an annoyance, to as much as 80% today," cites Goodman in one paper. Other experts estimate the percentage to be as high as 90%. With this increase in unsolicited mail, the war against spam has mirrored a conventional "arms race" scenario, where every countermeasure is matched or obviated by innovation or brute force

The common link between these two groups, the phishers and the spammers, is how they deliver their attack—email. Just as the "begging letters" of Dickens's day required an envelope and stamp, today's criminals need the ability to send email. The two camps come together in the class of spammer that uses spear-phishing to steal email accounts.

1.1. Spammers and Spear-Phishing

In 1994, almost as soon as the Internet was opened to commercial use, it began to carry waves of the unsolicited commercial message that, thanks to Monty Python, came to be called spam. In one of the most notorious early spam events, a pair of lawyers used the Internet discussion forum Usenet to propagate an advertisement for their questionable product, a guarantee of success in the Green Card Lottery offered to immigrants. Eventually disbarred, the pair tried to leverage their notoriety and "expertise" into an Internet marketing business—though burning through a number of Internet Service Providers, as well as their legal careers.

> *The couple claimed in a December 1994 interview to have gained 1,000 new clients and "made $100,000 off an ad that cost them only pennies."*

This event has been marked as "the spam that started it all," which led to the ever escalating battle between the spammers and their opponents, a conflict built on:

- the myth that spam is a wildly profitable enterprise;
- the platform of email, that allowed almost zero-cost propagation of fraudsters' mail solicitations;
- an increasing cycle of "over phishing" yielding more and more desperate spamming.

Here "phishing" refers to a type of spam aimed at gaining personally identifiable information sufficient to acquire financial resources from the victims. This is a specific category of spam that targets gullible recipients with the aim of defrauding them. Cormac Herley describes the desperate cycle driving the growth of phishing:

> *Suppose there were a fixed number of dollars available to be phished each year; that fixed pool would be divided among more and more people and each phisher's take would decrease. New entrants stop arriving only when the opportunity is no better than the opportunities elsewhere. So this argues that a fixed pool would be divided among a community of phishers that expands to drive the average return down.*
>
> *So far so obvious. However… the economics of phishing are far far worse than this. Rather than sharing a fixed pool of dollars phishing is subject to the tragedy of the commons... i.e. the pool of dollars shrinks as a result of the efforts of the phishers. A community (all phishers) share a finite resource (the pool of phishable dollars) that has limited ability to regenerate (dollars once phished are not available to other phishers). The tragedy of the commons is that the rational course of action for each individual (phisher) leads to over-exploitation and degradation of the resource (the phishable dollars).*
> [Herley, C. "A Profitless Endeavor"]

That illusion of gain is just that, an illusion. The relatively low cost of spamming in general means that anyone with an Internet connection can try it, so that there are many who compete for the harvest. This leads to depletion of the pool of available victims. As a result, phishers compete with each other, and against an array of opponents and technology. Such escalation is what has led to the dismal statistics that possibly as few as 1 in 10 emails is actually legitimate.

1.2. Attacks at Scale

In "The Plight of the Targeted Attacker in a World of Scale," Cormac Herley considers the economy of Internet attacks in terms of return on investment, analyzing the payoff of highly customized attacks compared to attacks at scale.

The customized attack is one directed against a high value target, and adapts to whatever defense is confronts. As a result, the overhead costs associated with the attack can grow without bound, or at least will grow until they've exhausted the defense budget of the target. This scenario is what might be called the classic "Mission Impossible" case, where the target must be taken at whatever cost is required and the attacker has unlimited resources. Herley describes this:

> *[The attacker] has many attacks that exploit vulnerabilities in [the target's] applications or operating system, her firewall, the network she uses or her susceptibility to social engineering. He even has techniques to spy on her using reflections from her LCD screen or audio or electromagnetic emanations. He constantly adds new attacks...*

Nevertheless, such an approach is beyond the means of most attackers on the Internet. Unless an attacker is backed by a corporation or nation-state, their campaign's cost will quickly outstrip any payback, as Herley notes:

> *No matter how clever the exploit, unless the expected value is high, there is little place for per-user effort in this world of mass-produced attacks.*

Facing such realities, most phishers will target not individuals, but broad populations. The 419 schemes or the credit union scam can be sent out indiscriminately. If there's no appreciable incremental cost for sending out one or 1,000 emails, why not send a million? Enough gullible victims can be harvested if one sends out enough email, so send out as much email as possible. This presents a resource problem.

While free email accounts are ubiquitous, they are not reliable to send mail at the volumes required by spammers. They are quickly closed when abused, and are not held in high regard as sources of serious commerce or "important security alerts."

Author: Joel Peter Anderson, joela@umn.edu

1.3. Schools of Phish: Spear-Phishing at Scale

If one decided to rob a bank, it is likely that one of the first considerations would be the getaway car. In addition, it is a good bet that a savvy criminal would make sure this car was not their own—they would probably steal one that could be easily dumped when the heist was complete. Likewise, anyone pursuing a career in criminal spamming will be looking for a means of swift and reliable transport. Transport equals email in this case, and they want accounts that are reliable, disposable, and not their own.

Large organizations, particularly large educational institutions, are perfect for spear-phishing attacks aimed at acquiring user credentials.

In the humorous business guide, *How to Succeed in Business Without Really Trying*, Shepherd Mead advises the aspiring executive to choose the right company: *"It must be BIG. In fact, the bigger the better. It should be big enough so that nobody knows exactly what anyone else is doing."* (p. 3)

Not a bad example of what the spear-phisher takes advantage of. The phisher doesn't have to worry about the effectiveness of the school's orientation process because there are always enough new people flowing through. Inevitably, there will be some who are too busy or who fail to closely examine the alarming messages sent by the phishers.

Figure 1: Proportional word cloud of alarming keywords from spear-phish received at the University of Minnesota.

Author: Joel Peter Anderson, joela@umn.edu

These stolen email accounts have a number of advantages:

1. Quantity – every school has a guaranteed annual turnover with each new class that enters.
2. Naiveté – the phisher is looking for novice users, likely unfamiliar with the institution's systems and rules who are ripe targets for their deception.
3. Trust – unlike obviously free accounts (hotmail, yahoo, gmail) email associated with institutions of higher education are more likely to seem legitimate.
4. Validity – by coming from an accredited institution, automated measures like Sender Policy Framework (SPF) and DNS checking will fail to prevent the delivery of the spam sent from the compromised account.
5. Disposability – it doesn't matter to the spammer when their hijacking of the account is detected. There are more accounts available all the time (see point number one).

These factors aren't limited to colleges and universities, but such institutions easily contain the key characteristics for successful mass-market spear-phishers in choosing a target.

The appeal of universities and other higher education institutions to phishers became apparent around 2008, when email system administrators began to compare notes about scams they were seeing hit their schools. SecurityFocus noted:

> *In an ongoing attack, students and faculty at nearly a dozen universities and colleges have been targeted by phishing e-mails since the middle of January [2008]. The e-mail messages masquerade as missives from each school's help desk, asking that the student confirm their username and password as well as requesting more personal information, including date of birth and country of origin.*

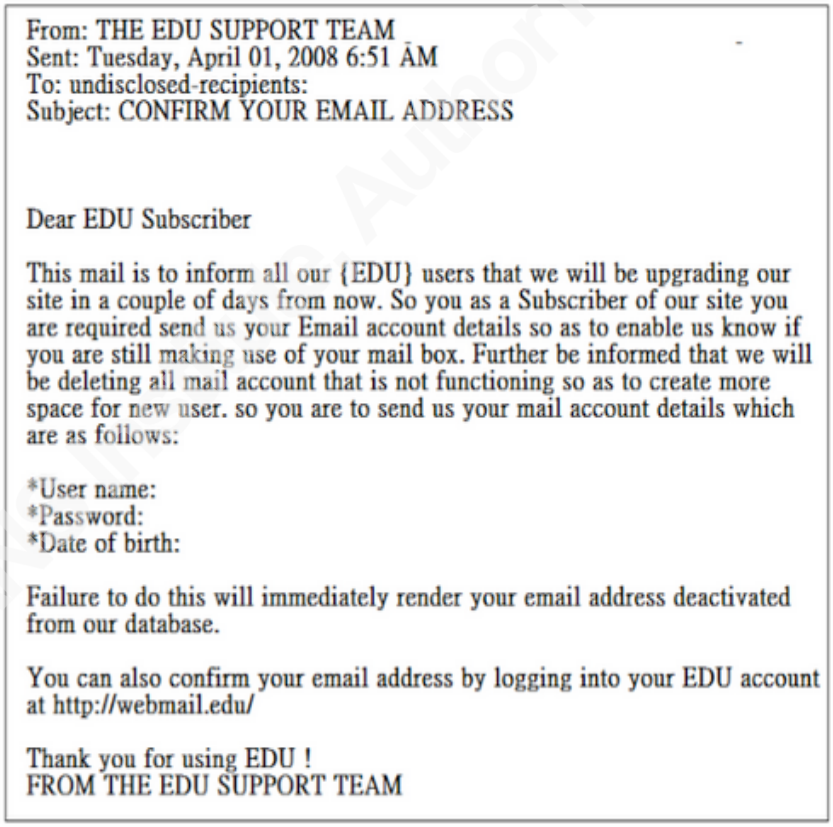
The university where I work was one of these and we began to observe a pattern. An account would suddenly blast out hundreds, even thousands, of spam messages. Rarely would we see these messages sent TO people at our school—presumably hoping to avoid notice. We would learn of it from the side effects.

Author: Joel Peter Anderson, joela@umn.edu

The consequences of a compromised account were people accusing the school of spamming or complaining about a misbehaving student engaged in fraud. Users who had been compromised would complain about discovering their inboxes full of bounced message they hadn't sent (most spammers don't bother to carefully curate their lists of potential victims).

Adding threshold limits to how much email a user could send in a short time helped detect the compromised accounts, but at first, it wasn't clear how the accounts were being taken. Without any evidence, we didn't know if they had lost their password to a virus, scam, or an infected compromised computer.

Then we started getting reports of phishing messages that our users were receiving (yes, the following really came on April Fool's Day):



From: THE EDU SUPPORT TEAM
Sent: Tuesday, April 01, 2008 6:51 AM
To: undisclosed-recipients:
Subject: CONFIRM YOUR EMAIL ADDRESS

Dear EDU Subscriber

This mail is to inform all our {EDU} users that we will be upgrading our site in a couple of days from now. So you as a Subscriber of our site you are required send us your Email account details so as to enable us know if you are still making use of your mail box. Further be informed that we will be deleting all mail account that is not functioning so as to create more space for new user. so you are to send us your mail account details which are as follows:

*User name:
*Password:
*Date of birth:

Failure to do this will immediately render your email address deactivated from our database.

You can also confirm your email address by logging into your EDU account at http://webmail.edu/

Thank you for using EDU !
FROM THE EDU SUPPORT TEAM

Figure 1: Early spear-phishing received at the University of Minnesota

Essentially a request to "please tell us your name and password," these messages were effective enough to require us to develop protocols to deal with them. We established an email address to send reports of such messages. We set up tools to quickly block the reply addresses. Members of the Email Administration in Higher

Education listserv spun off a group, eventually set up as an independent Google group (APER, the Anti-Phishing Email Response group), to track and report on the sources of these spam. With collaboration, we could anticipate or block email from the many sources—often compromised accounts—and block replies to the fraudulent messages.

The APER group developed a taxonomy to categorize the email addresses contained in the messages. Email addresses were categorized as to whether they were the "reply-to" address intended to capture responses, whether they were obscured in the message headers, whether they were in the text, or whether they were "errors"—email addresses that were meaningless—either non-functional, or not able to receive replies.

Over time, it became apparent the strategy was changing. Reducing the address types to two categories, reply-to and error (that is, an email address not intended for replies), it is clear that the original "form letter" approach was being abandoned. Looking at the cumulative data from APER, this trend became clear when graphed:

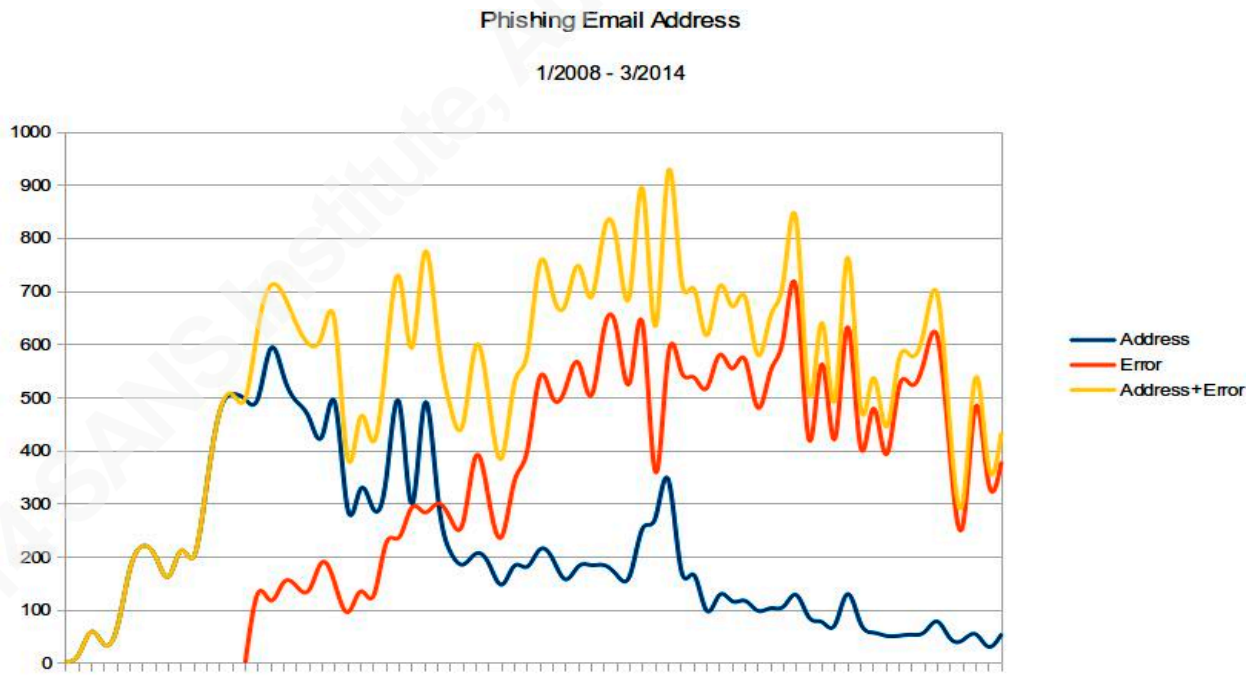


Figure 2: Spear-phisher Address Types (APER data, graphed by author)

As time went on the number of email addresses that were intended to accept a response sloped closer and closer to, but not yet reaching, zero. Meanwhile, the "error" addresses (bogus, non-functional, or otherwise not intended to receive replies) became the norm. So how were the phishers collecting results? By using forms!

Author: Joel Peter Anderson, joela@umn.edu

A number of locations on the Internet provide a "free web form" function, much like the free webmail services that have proliferated. These services offer a simple mechanism for users to create forms for any purpose, legitimate or not. Depending on the skills and effort the spear-phishers were willing to expend, the forms sent to our university were a mixed bag.

Using these tools, some of the spear-phishers would add images they had discovered on the Internet to add some simple branding to their pages. While not conforming to standard university templates, with these they attempted to strengthen their claim to be from the University of Minnesota.

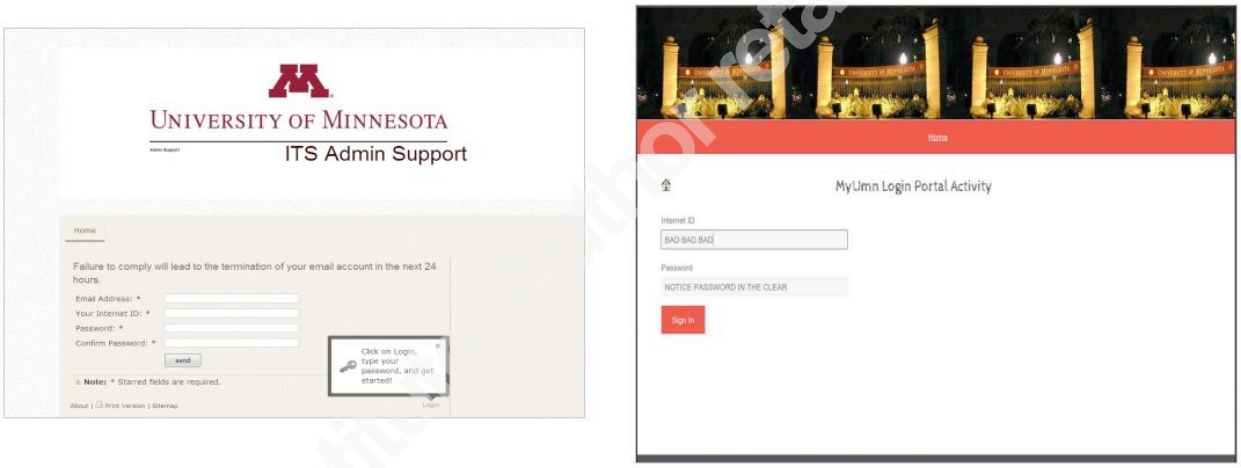


Figure 3: Weakly branded form set up on free provider (received at the University of Minnesota)

In contrast to this, many of the forms are completely generic, with no reference at all to the target institution. While this undercuts their plausibility, it may still serve their purposes. Remember, these campaigns are conducted at scale, often against multiple targets. It is simpler to produce a form that is generic and can be directed to more than one school.

Author: Joel Peter Anderson, joela@umn.edu

Figure 4: Non-branded Phisher forms (received at the University of Minnesota)

More capable phishers set up their own servers, or borrow compromised ones, and create counterfeit pages that look like, or very close to, the real thing:

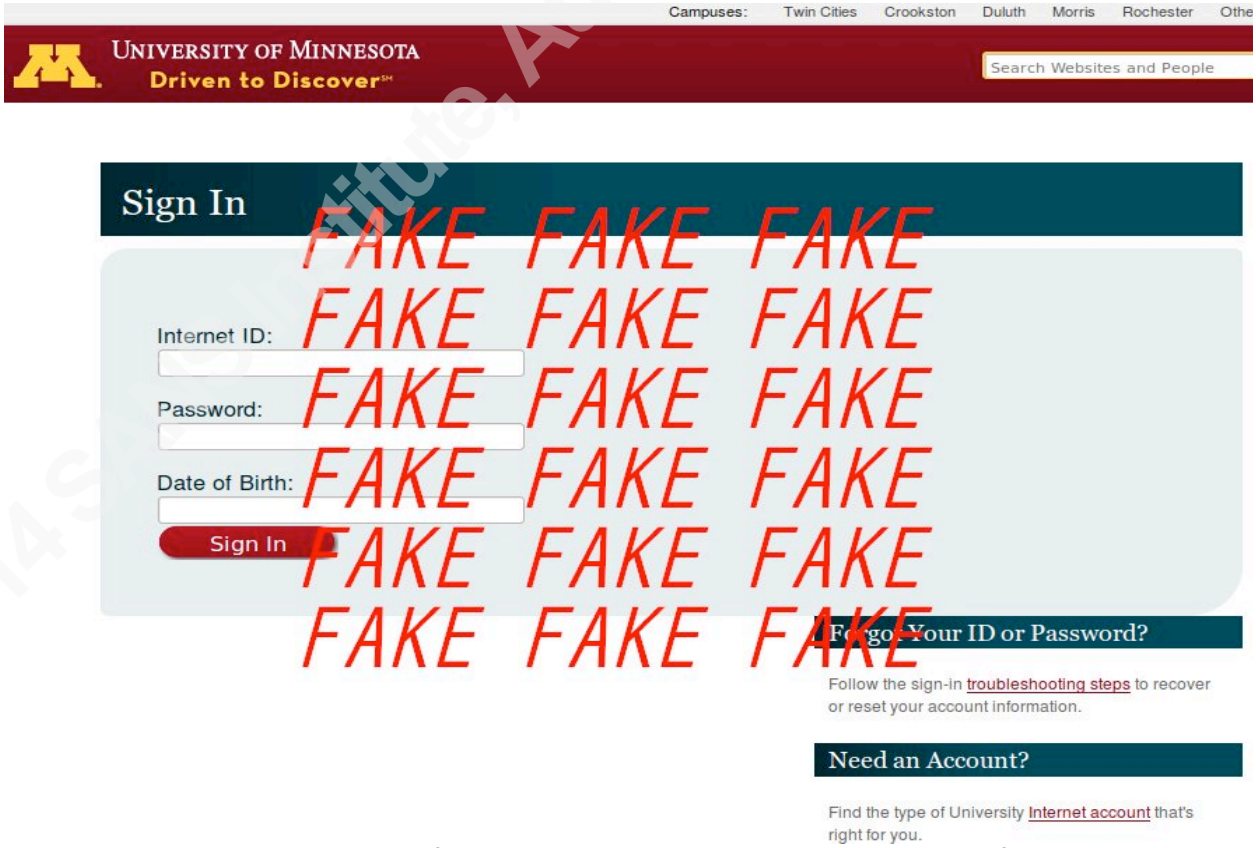


Figure 5: Phishing form that (mostly) accurately copies a real login form

Author: Joel Peter Anderson, joela@umn.edu

Legitimate companies providing web forms generally *are* responsive to requests when phishing is reported. Most have contact forms to make such reports, with an option to make clear that a phishing form is being reported. In 2013, after Oxford University had blocked Google Docs from their network, Google modified the forms provided by the Google Docs product to explicitly warn against using their forms to submit passwords (note: the example Google form in Figure 4 pre-dates the addition of this warning).

With this change, Google forms now displays a warning that explicitly warns the user, "Never submit passwords through Google Forms," as can be seen in this example:

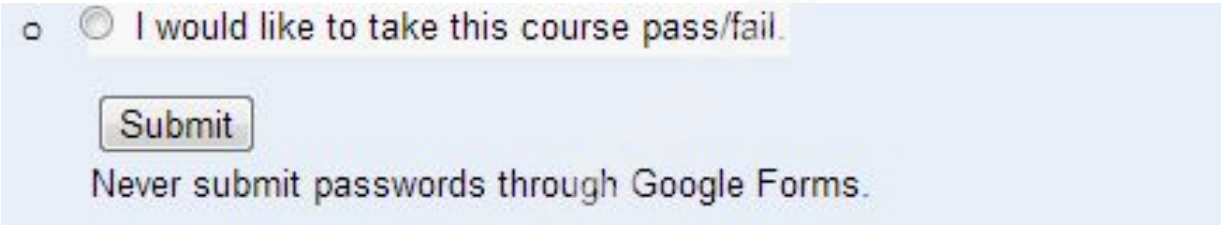


Figure 6: Google form with password warning (from a columbia.edu course registration form)

That simple change had a dramatic effect on the free form provider choice made by spammers, as could be seen examining the phishing links reported by the Anti-Phising Email Response (APER) group:

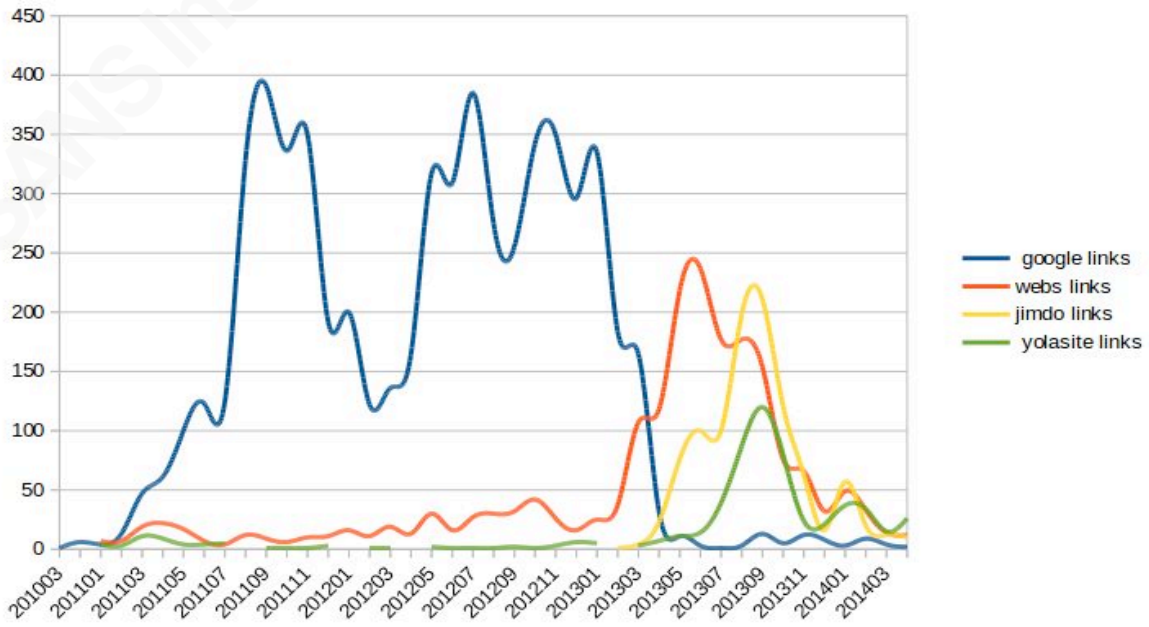


Figure 7: Use of Google Forms for phishing dramatically declined with the addition of their password warning (APER data)

Once Google started warning people against putting passwords in their forms the number of Google forms plummeted, and as can be seen, the other major form suppliers took up the slack.

1.4. Is This Really A Problem?

Who cares? Before even trying to address this issue, is it a problem that matters? In a word, yes.

Stealing email accounts is a crime with many potential payoffs. Brian Krebs detailed this in a useful diagram:

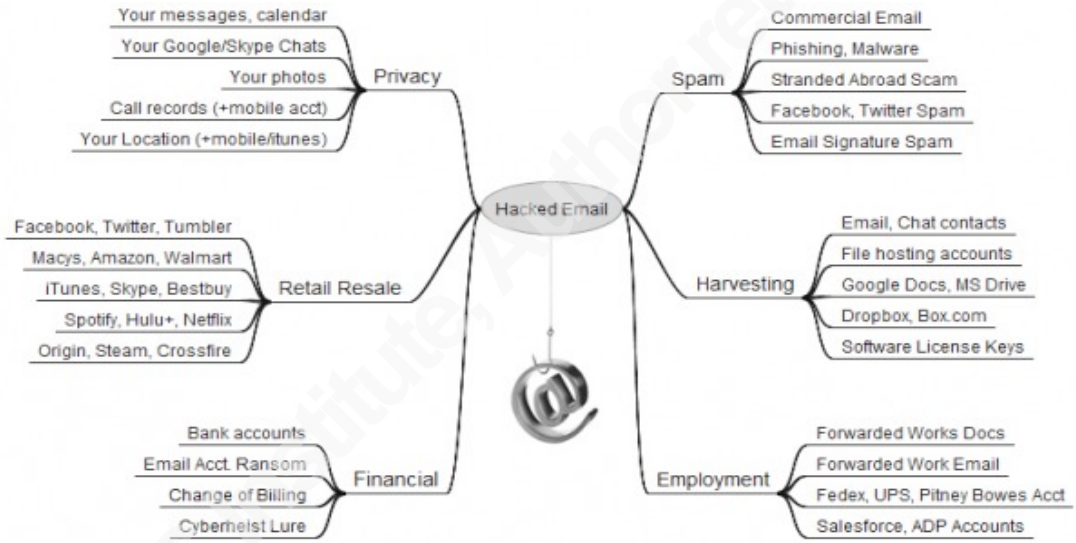


Figure 8: Krebs, "The Value of a Hacked Email Account" (krebsonsecurity.com)

At our school and others, the main payoff appears to be the ability to drive spam campaigns, but that may be because it is the noisiest aspect of account hijacks. Sending spam from a hijacked account generates many side effects: bounced emails, complaints, blacklisting by other mail systems. Other uses of the stolen account—for example, browsing university licensed library content—may happen at a low enough level that no one notices.

Password reuse means that the compromise of ONE account may lead to multiple accounts being hijacked. The frequent use of "email address" as login identity means any number of valuable assets can be lost in one password exposure event.

Author: Joel Peter Anderson, joela@umn.edu

Password dumps that have been reported to our organization have included university credentials, even though the dump came from some unrelated site.[1]

While the use of accounts for spamming is the most noticeable abuse, the potential exists for much more serious consequences within an organization.

First, simply sending email *within* the organization—to all the contacts in a person's contacts list—is an effective way to capture accounts. An attacker, using a compromised account will send an email that says, "I've shared a document with you" with a link to a form like this:

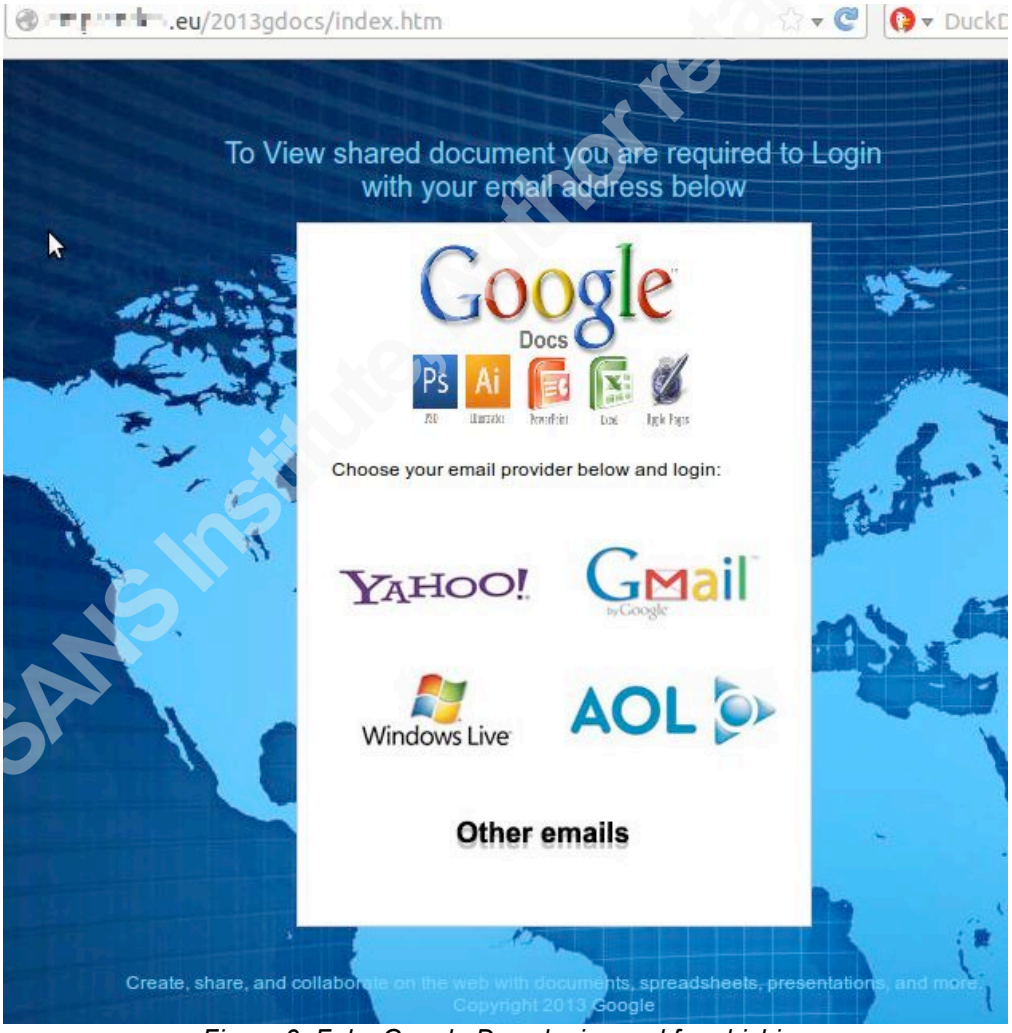


Figure 9: Fake Google Docs login used for phishing

1 Such reports come from a variety of sources, for example higher education consortiums that monitor dumping sites for .edu credentials.

Author: Joel Peter Anderson, joela@umn.edu

It does not matter that this does not really look like a Google Docs share; there are enough people within a large organization unfamiliar with the correct interface. If the compromised sender is important enough and people feel obligated to follow the link, such an appeal can capture quite a few accounts.

Since many organizations have worked towards "single-sign-on" (one ID and password for all organization logins), subverting an email account often means important things, like direct-deposit settings, can be modified once a user's ID and password are known. This has been reported at some schools.

2. Fighting the Phish - The Road Toward Reducing "The Catch"

As our response to spear-phishing evolved, we found that developing a response to the onslaught of spear-phishing should proceed on three levels.

1. Incident Response – recognizing there will be successful attacks.
2. Access Control – imposing controls to prevent/mitigate account compromise.
3. Advanced Discovery – developing information to adapt and improve activity to control and response activities.

Author: Joel Peter Anderson, joela@umn.edu

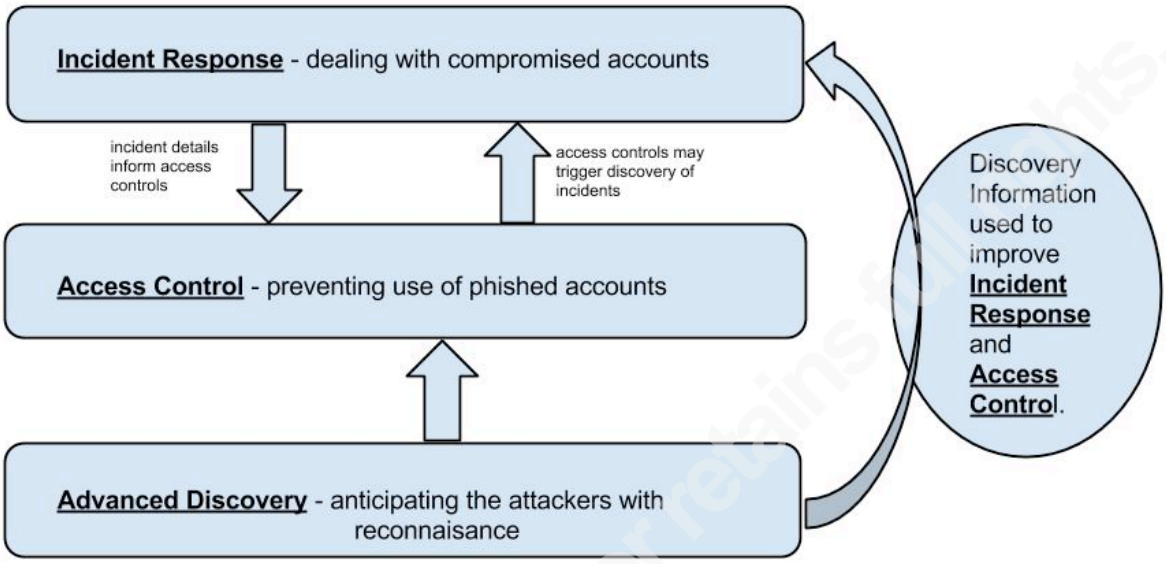


Figure 10: Three levels of spear-phishing response

2.1. Incident Response

Incident response stands as the foundation of any program to reduce the spear-phishers catch.

First, as with many problems, the first step is admitting you have a problem. Spear-phishing IS going to happen. Unless you have absolute control over user behavior, people *will* give up authentication credentials and you will need to be prepared with the correct response.

Second, being prepared with a systematic response to phished accounts will allow your team to contain and mitigate the consequences of the incident.

Finally, your incident response team should be prepared to harvest relevant information from each event to aid in detecting—and better, *preventing*—future compromises.

Author: Joel Peter Anderson, joela@umn.edu

Our response to a compromised account has three parts: quarantine, recover and profile:

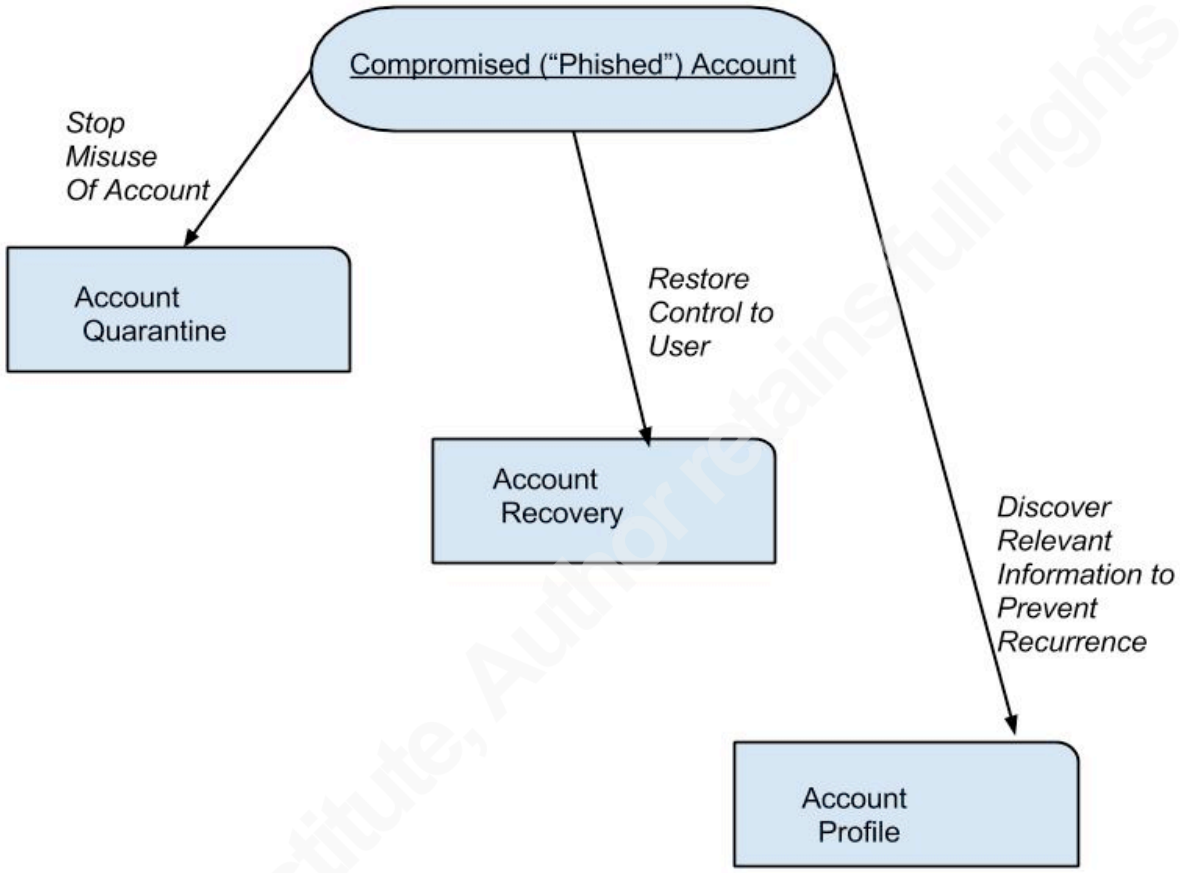


Figure 11: Handling phished accounts

2.1.1. Account Quarantine

With the discovery of a compromised account, all access and privileges need to be locked down as soon as possible. This is the advantage of single sign-on authentication. Locking the account will stop continued misuse and give you an opportunity to recover the account.

Authentication cookies need to be revoked to prevent continued use of the account. It is not enough to just change/scramble a user password. For example, if the attacker is actively using a webmail account, they may be able to continue to use the hijacked account. You must be prepared to restrict all account activity in the event of compromise.

2.1.2. Account Recovery

Restoring access to the compromised account is the next step. Coordinating incident response with front-line service personnel means that you need to document the incident ("account [username] was phished") so that the help staff can explain the incident to the user, and assist them with recovering control of their account. Help staff needs to be prepared to assist in discovering if the attacker has changed user information, set up auto forwarding from the account, or modified user "secrets" used to reset a password.

Some user populations, such as when a university allows alumni to retain their email accounts, may have marginally affiliated users. These people can be good targets for the spear-phisher because they may not pay close attention to their university account. Assisting this user population can be a challenge because the institution's contact information (phone numbers, student address) may no longer be current. In a similar way, new students are increasingly *less* likely to want to use their institutionally provided email; they usually have an account they've used for years and have no intention of using the school's system. When compromised, they may be slow to notice because they are not using the account.

For an organization that has employee accounts, which may become compromised, the recovery process must include informing relevant people to ensure that there are no extraordinary consequences. This includes notifying information technology staff that support the compromised employee, as well as other departments that may need to be alerted. In our experience with this problem, the majority of attacks are aimed mainly at taking over email accounts for spamming, along with accessing licensed resources (e.g. library publications). However, as noted earlier, some institutions report direct deposit settings being changed, which results in paycheck or reimbursement diversion to attackers' accounts when a user's password has been acquired. A good precaution for responders to the compromise of employee accounts is to alert payroll to review user account activity.

Our process in handling a compromised account follows these steps:

- **Close account immediately;**
- **Inspection of the account details** to determine whether the account has been modified (e.g. if forwards have been set, secrets changed);
- **Clear login cookies** when possible;

Author: Joel Peter Anderson, joela@umn.edu

- **Re-open of the account** [the close/open in our system will clear secrets and forwarding, as well as scramble the password];
- **Log the compromise event** for front line service personnel—they need to be informed when the compromised user calls in;
- **Notify the staff support** for any current employees who are compromised;
- **Notify the payroll department** (if the user is a current employee) to review account activity;
- **Send email to the compromised user** (note: this will be only available after they have recovered access to the account with the assistance of the front line service personnel or the user's support staff);
- **Security review of all account activity** for information about the attack source.

2.1.3. Account Profile

This final step involves profiling the account activity, and is intended to discover relevant information to discover/prevent future attacks. This relies on access to relevant log information, including, but not restricted to authentication events, mail queue logs and remote access (e.g. Virtual Private Network [VPN], wireless) records. This can assist in identifying events of compromise, and discovering misuse of accounts.

With an account compromise, your system logs can yield clues that will help detect and prevent future events:

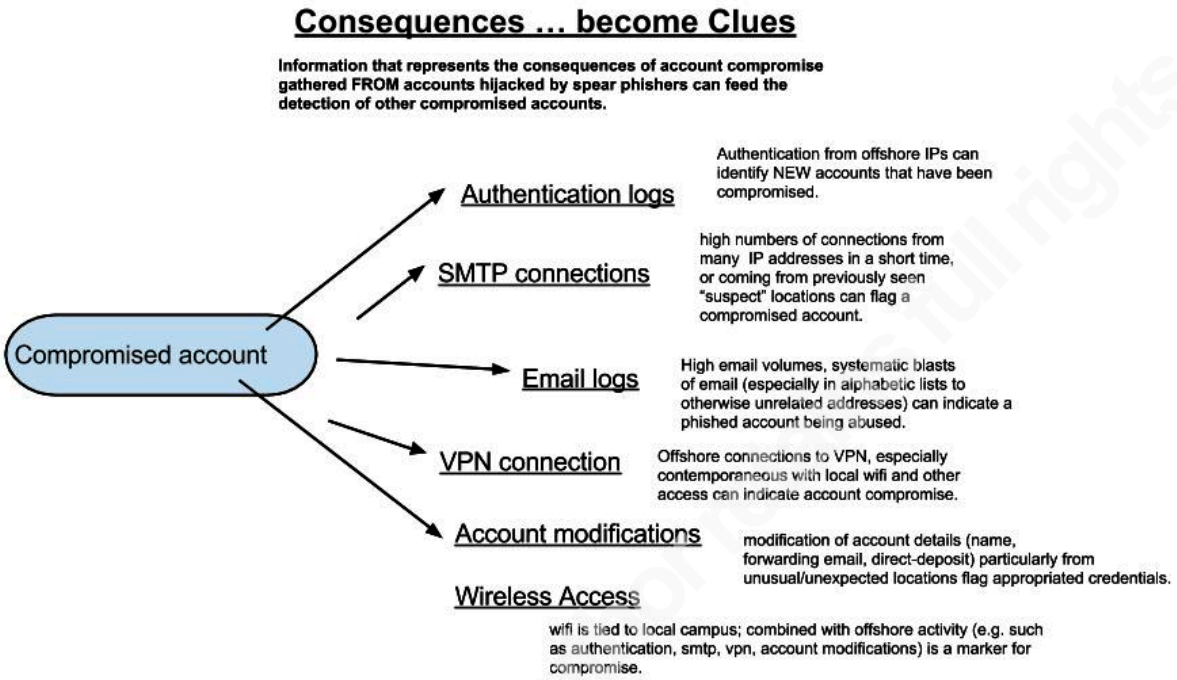


Figure 12: Profile compromised account for improved access control

Following an account compromise, we review account activity to harvest useful information:

- **Authentication events** – identify offshore IP addresses that may source future compromises;
- **SMTP connections** – identify IP sources used; can uncover other compromised accounts;
- **VPN activity** – compared with other known activity can flag compromised users; collecting origination IPs flag activity on other compromised accounts;
- **Account Modifications** – identify activity to be triggering on for new attacks;
- **Wireless Access** – requires local presence; tied with logging of access from foreign locations flags compromised accounts.

Information gleaned from incidents is used in tuning access controls that are used to prevent or detect new attacks.

Author: Joel Peter Anderson, joela@umn.edu

2.2. Access Control

Imposing controls to prevent/mitigate account compromise, i.e., access control, can be key to the prevention of compromise via stolen credentials. Controls that prevent the use of credentials provide an active barrier to attackers, while using ongoing audit logs provide a means to passively detect activity that needs to be investigated and dealt with.

Controls may be active, imposing measures that prevent access and misuse by attackers through hardware or software tools, or passive, using ongoing monitoring to alert on threat activity:

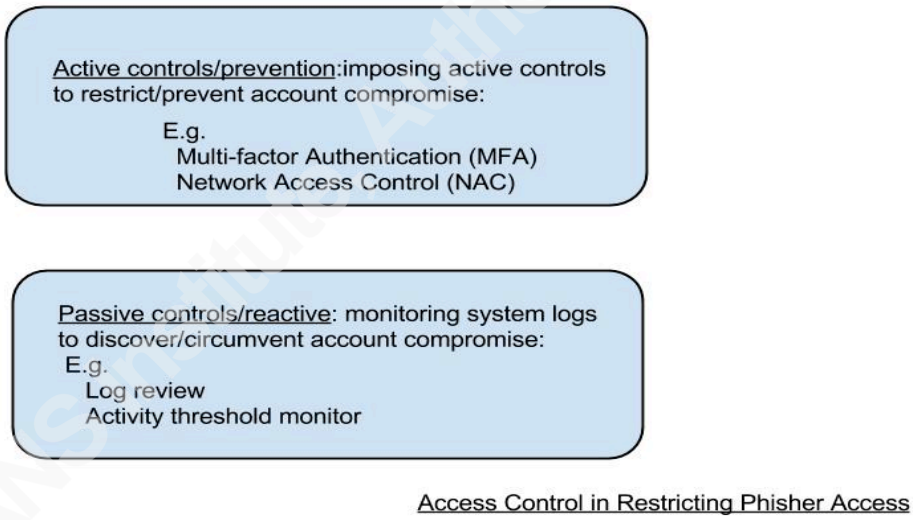


Figure 13: Access Control - Active and Passive

2.2.1. Active Controls/Prevention

It seems axiomatic that hijacking accounts could be effectively stopped if simple passwords were replaced or augmented with two-factor (or multi-factor) authentication. While there are attacks that can bypass two-factor authentications, when logins require "something you know" plus "something you have," this stronger authentication mechanism can diminish the ability of spear-phishers to acquire useful credentials.

Multi-factor authentication methods (e.g. Duo, RSA SecureID, Yubikey) are being adopted, but slowly. A major barrier is the cost in resources, both financial and organizational: implementation requires adopting a system *and* dedicating the personnel to support it, *AND* training people to use the service. The support and training required to get such a system running alone are a significant deterrent. If the prospect of compromised accounts is not seen as enough of a risk, the complexity of implementing multi-factor authentication will prevent widespread adoption of multi-factor authentication.

Because simple passwords are easy to use and easy to implement, two factor authentication tends to be limited at present to opt-in choices (e.g., Google, Yahoo, Twitter, and other services allow, but don't mandate it) or as mandated for high-value operations (e.g. system administrators, or tightly audited "secure" systems).

Likewise, using Network Access Control (NAC), a "policy-enforcement mechanism originally designed to authenticate and authorize systems attempting to connect to a network" can be a powerful tool in preventing the compromise of accounts via phishing. As one vendor described NAC:

> *Network Access Control (NAC) solutions protect organizations, and enforce corporate policies to keep devices configured correctly and operating at top efficiency. NAC solutions verify protection against viruses, spyware and other security threats that are transmitted via networks and network-enabled applications, or that take advantage of unpatched vulnerabilities in operating systems and applications*. [netmotionwireless.com]

Again, as with multi-factor authentication, NAC solutions are not universally deployed, for many of the many of the same reasons. Writing in Network World, Joel Snyder noted barriers (*"...politics gets in the way, too many vendor variations, interoperability woes deployment difficulties, hidden scalability issues, and ROI is not balanced with cost..."*) that make it difficult to find NAC used in a large, diverse organizations such as the colleges and universities that are plagued with spear-phishing.

It is appealing to impose active controls—strong, automated policy enforcement on access—but the implementation of this may not be available or practical for every institution. This is why there is an advantage in developing passive reconnaissance tools to discover violations and abuse of accounts. Audit logs for resources, authentication events, and more can be used to discover and respond to the misuse

Author: Joel Peter Anderson, joela@umn.edu

of account credentials. If you're already logging activity (as you *should* be), you have the data available that can be built into a solid means of reducing the catch of the phishers.

2.2.2. Passive Controls: Using What You Already Know

Audit controls are more than a check-mark to satisfy compliance goals. By building automation around existing logs you can discover compromised accounts and prevent them from doing damage instead of cleaning up after the fact.

As noted earlier, profiling activity in a compromise using a review of system logs will provide data to develop triggers that can alert regarding compromised accounts for incident response at the earliest moment.

The GULP system developed at Columbia University is a good model for building on the existing collections of data in a coordinated manner. As a tool for aggregating network logs, GULP provides resources for many aspects of managing resources, including activity that indicates account compromise, as this figure shows:

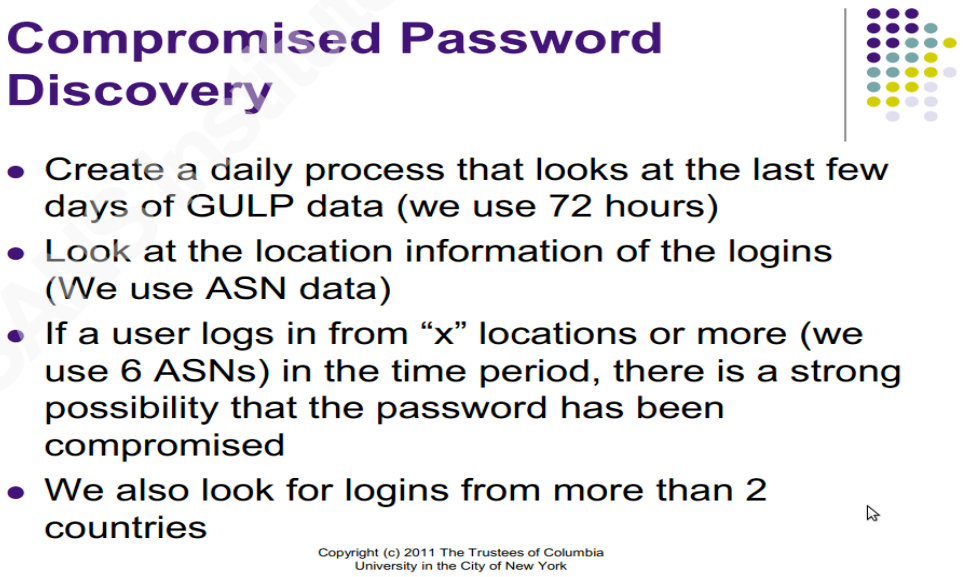


Figure 14: Using logged data to discover, circumvent compromised accounts. (nysernet.org)

GULP is described as, "a flexible aggregation system for authentication log data. The system merges disparate logs stored across various servers into a single format according to an XML schema. This single format is logged to a database and queried

via a web interface. The strength of this system lies in the ability to correlate information across multiple logging sources and display relevant information through a simple interface." Such a tool has multiple applications, but the relevant use for this discussion is the use as a control to discover account misuse, and a driver to incident response.

Considering logged information available within our environment, this diagram summarizes how my university has used it to detect and respond to compromised accounts:

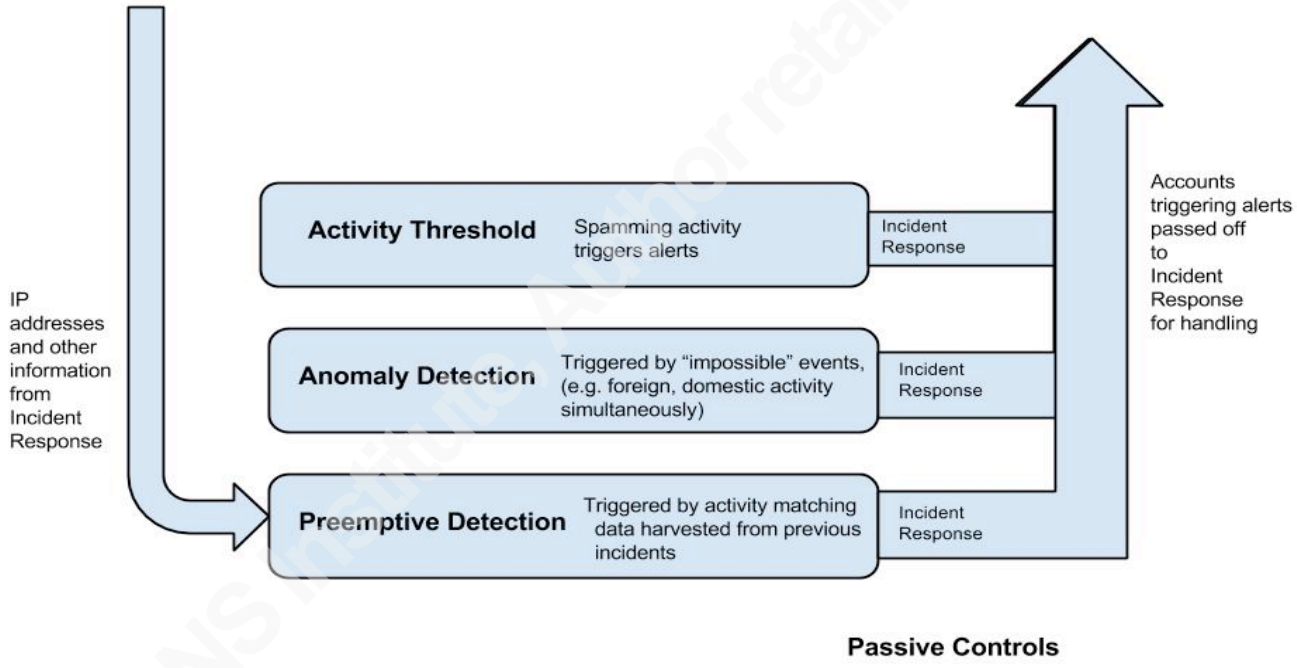


Figure 15: Passive controls used to detect/mitigate phished accounts

Our university has focused on three strategies for implementing passive controls: activity threshold, anomaly detection, and preemptive detection.

Activity Threshold

Currently the focus of known spear-phishing attacks appears to be harvesting email accounts for use in spamming campaigns. Because of this, the administrators of our organization's email system have established thresholds that are tight enough to interrupt compromised account spamming events. Discovery of an account that triggers threshold alerts sets into action immediate closure of the suspect account. The quota is flexible, and has been developed over time. Also, there is a whitelist to exempt accounts permitted to send higher than normal email accounts.

Email from the specific accounts is quarantined to prevent delivery, and the event is reported to the security team. Security analysts follow the incident response steps detailed earlier. Important in these events is profiling account activity, as noted earlier. The data from the profile can be used to identify phisher Internet addresses, which are used in the preemptive strategy (below).

Anomaly Detection

Anomaly detection establishes controls that systematically review user activity and triggers on improbable (or contradictory) events. Quick identification of users apparently coming from geographically distant locations simultaneously is a good trigger and can discover account compromise (as well as inappropriate sharing of accounts). Tools like Columbia's GULP and Splunk are being used to identify anomalous events and discover credential theft.

We've developed an automated system that uses data from specific network resources recognized as a popular target for misuse. The activity targeted *is* legitimate for account holders, but can be easily flagged for inspection.

Once a day:

- An automated process identifies targeted activity originating from offshore locations in a 24 hour window;
- A list is compiled of accounts from those locations accessing the network in that time frame;

Author: Joel Peter Anderson, joela@umn.edu

- Finally, an aggregate profile of activity from each account is compiled, flagging accounts that are "bi-located," i.e., simultaneously on our local network and coming from a distant network.

Accounts identified are handed over to incident response. Analysts review activity and process the event as noted earlier. In addition to discovering compromised accounts, this process identifies active sources (i.e. IP addresses) for attack activity, which can be added to a preemptive detection process.

Preemptive Detection

Initially, we attempted to identify subnet ranges known to host high activity by the phishers. An automated process flagging authentication events could then be used to discover compromised accounts. While useful, it was too wide a net and had many false positives—it was common to have professors and students traveling in these regions. Since we have international members of our university community, it was perfectly reasonable that there would be activity originating within those networks.

Our alternative was to focus on individual addresses. We began to compile a list of Internet addresses from which successful phishers had launched runs on our network. While this was not without false positives, we were able to discover newly compromised accounts, and prevent activity before it began. Significant in ruling out false positives was the ability to audit current activity by any (possibly) compromised account. When an alert is triggered a report is given to our incident response team that includes all current activity—travelers stand out from the compromised because the compromised tend to have recent domestic activity mixed with the attackers offshore activity.

Building off this model, we began to build a similarly curated list of network locations used to borrow VPN access. Again, the VPN service is a legitimate resource for staff and students to use when off our local network. It's a security measure when you are connected from an insecure network, and also provides access to network facilities not accessible off the local network. This last point makes it attractive to attackers who want access to things within our network, as well as to gain a launching point to obfuscate their location before launching an attack.

One incidental means of discovering compromised accounts is from intrusion detection of infected systems. Attackers who are borrowing university resources via

VPN may be operating from systems that are infected, which means that intrusion detection systems can spot them and have them isolated from our network. This may then confuse the innocent users whose accounts were compromised: "My VPN session is infected? What *IS* VPN?" Reviewing the activity we would then note the source address was foreign, and gain another offshore address to add to our detection process.

This process, when used to discover compromised accounts is cumulative—the discovery of a compromised user triggers an incident. As part of the follow-through process, account profiling will capture more IP addresses, adding to the preemptive process and potentially discovering new compromised accounts.

2.3. Advanced Discovery

The final piece we use to reduce the catch of spear-phishers is a process of advanced discovery; i.e., discovering potential access addresses in advance.

A common type of phishing form for a number of years was the PHP Formgenerator. The popularity of this can be seen reviewing the number of URLs reported by the APER team. In 2011, there was a peak of over 45% reported URLs using this PHP tool. While the reasons for this choice are not known (guesses include badly secured PHP Formgenerator installations or insecure webservers to which an attacker could easily add the form tool) the installations revealed some things about the phishing process.

Tallying the URLs reported logged by the APER group, and comparing them to the other web links used for phishing, this graph shows the growth and decline of the use of this tool for building spear-phish websites:

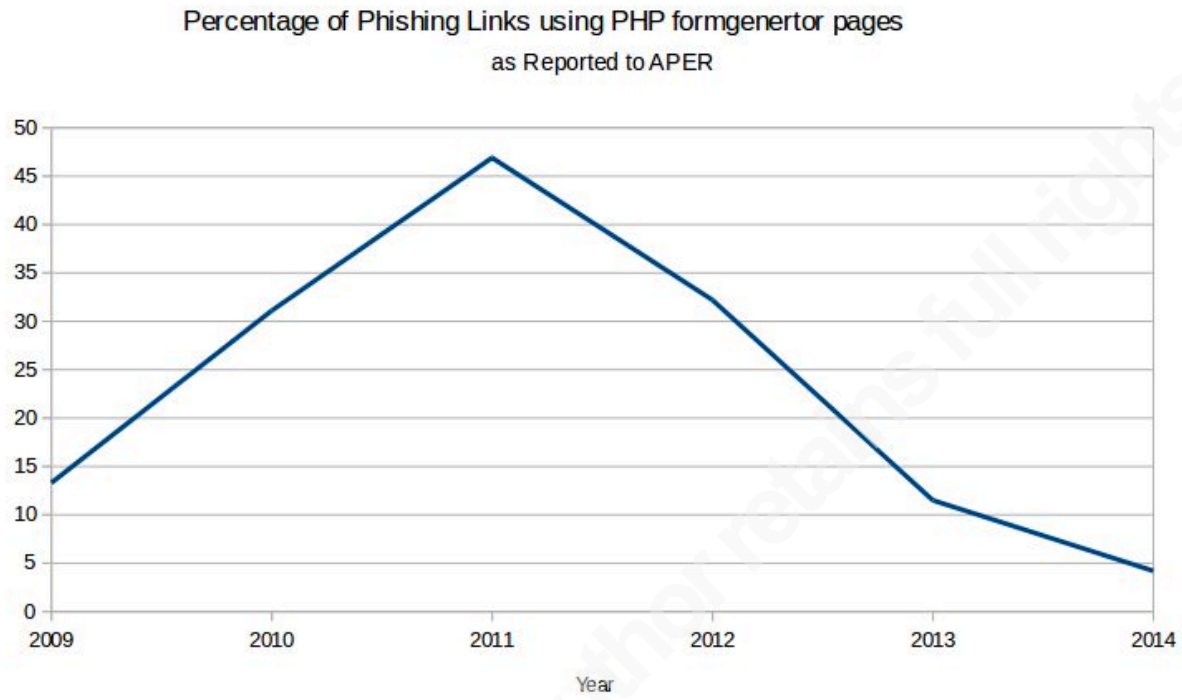


Figure 16: Percentage of forms reported to the APER group using PHP Formgenerator

Most sites set up with this software were extremely simple so it's not surprising that as better form tools became available, especially free webform providers, the drop-off in use of PHP Formgenerator was inevitable.

Many of these forms were extremely simple, devoid of any sort of customization, as can be seen in this example:

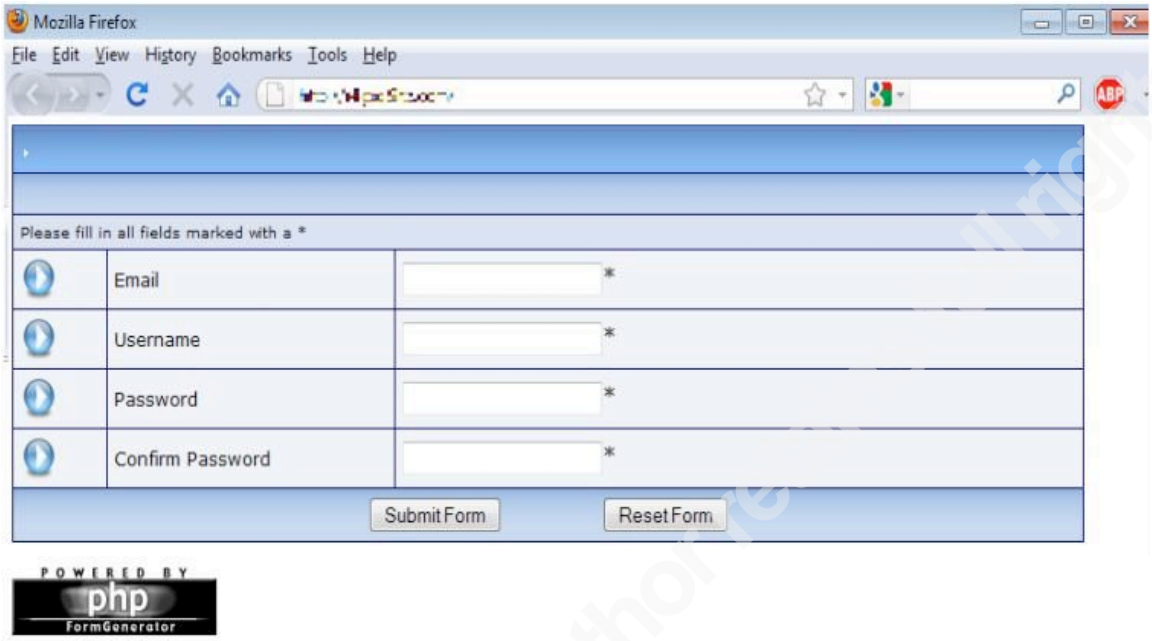


Figure 17: Example of a simple phishing form created with PHP formGenerator (m86security.com)

These forms were interesting because investigators could easily follow them back to their source. One researcher observed:

> *The administration pages for... the ... phishing forms were also freely available after a bit of digging, and this was what was found on the admin page corresponding with the scam targeting education institute members (Note each email address ending in .edu)* [in the figure below]:

Records Table

Full Names	Email Address	User Name	Password	Confirm Password	Delete Record	Printer Friendly
	.edu				delete	Print
					delete	Print
					delete	Print
	.edu				delete	Print
	.edu				delete	Print
	.edu				delete	Print
	.edu				delete	Print
	.edu				delete	Print
	.edu				delete	Print
	.edu				delete	Print

Figure 18: Administrator page on a phisher created formgen web page (m86security.com)

In this author's experience, viewing these forms and the admin pages behind them, many were noisy—cluttered with responses ranging from trivial and silly to insulting and vulgar. Along with that clutter, there were clearly responses from gullible people who had been deceived. The conclusion: it falls on the phisher to sift through such messy data and test it to find out if it is valid. From this insight, we began to work with what we referred to as "honeypeeps," a neologism from the "honeypot," plus "peep" for people—essentially false identities created to send to phishers.

Generating a pool of honeypeep identities, we had a resource that could be used and tracked to see if our responses to phishing would identify network addresses that we could in turn monitor for future attacks. What we needed were forms to put these honeypeeps into, but that was something we had.

In our communications with our user community, we advise them to report phishing attempts. This gives us a regular collection of new attempts to phish user

accounts. Incident coordinators follow a standard process with reported phishing attempts:

Old phish:

- **Log and thank** for reports of known phish.

New phish:

- **Log and promise to block;**
- **Block email** replies to phish;
- **Block network address** of phishing forms;
- **Report phishing form** to host company (when reputable);
- **Report to Anti Phishing Email Response** (APER) group.

With regular reports of phishing, and the actions we took to block them, we recognized we could take advantage of the phishing forms and seed the honeypeep IDs to see what happened.

Our process in using this tool is outlined with this diagram:

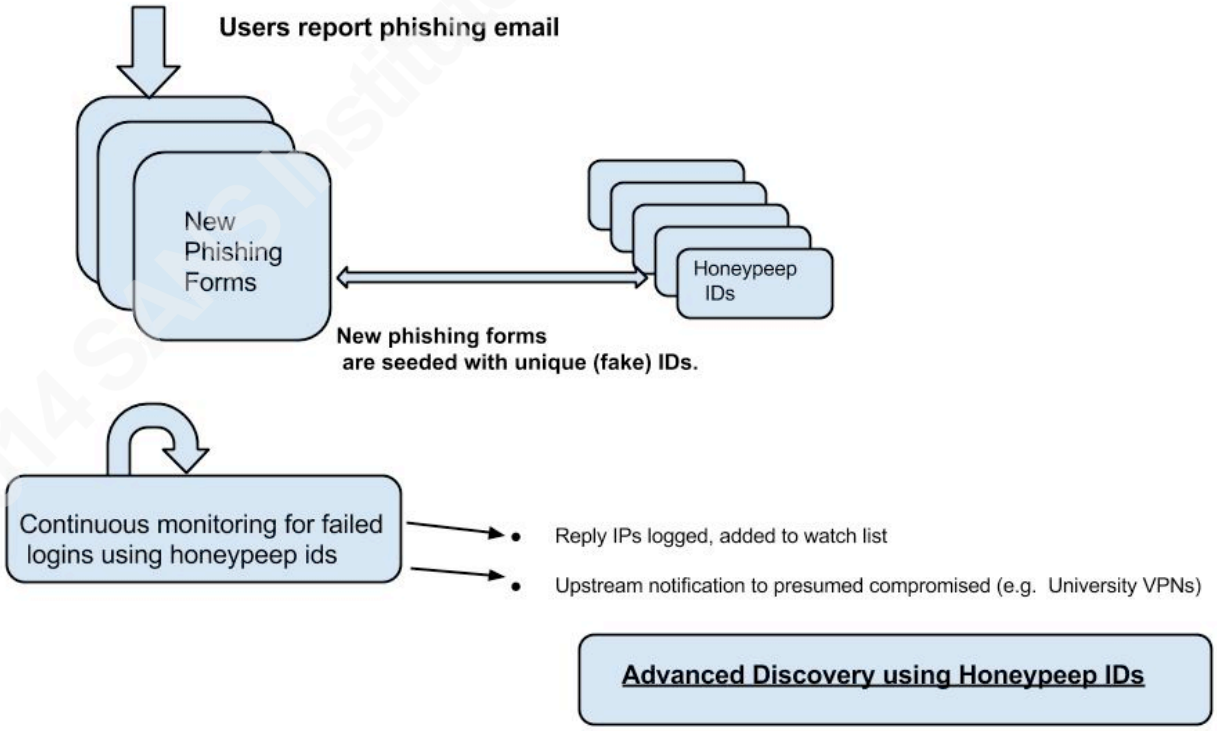


Figure 19: Using honeypeep IDs to discover phisher activity

Author: Joel Peter Anderson, joela@umn.edu

This was a gamble with no guaranteed payoff, but it has worked well. At present, our return rate is almost 57% of all addresses sent out. We have gained many addresses to add to our discovery lists, and discovered compromised accounts that were accessed from the newly discovered phisher addresses. We have also gained a number of insights into the activities of the phisher community.

To date, our replies come from almost two dozen countries. It is no surprise that there is significant representation from locations in the AFRINIC (the regional Internet registry for Africa) and APNIC (Internet registry that serves the Asia Pacific) regions, though there are a number from the US and European domains. In some cases we surmise these are compromised accounts (e.g. when .edu domains are the source) and in others there is possible use of purchased (or stolen) access from commercial providers offering VPN services.

Responses when they come can be *very* prompt. Fifty-five percent come in the first two days after sending out a honeypeep ID, and 69% within the first ten days. On the other hand, the honeypeep addresses have a surprising shelf-life. Some have been responded to again and again, suggesting that the phishing community trades lists, passing them on without any review.

It's also apparent that some may be captured without use for a long time. We have seen IDs that were held for 8 months before being used, and another that was used immediately, then two more times, 0 days, 9 days and a record 352 days after the address was sent to the phishers.

After more than a year sending out the honeypeeps, we can graph the response time to illustrate both how quickly the phishers use them, and how very long they hang around:

Author: Joel Peter Anderson, joela@umn.edu

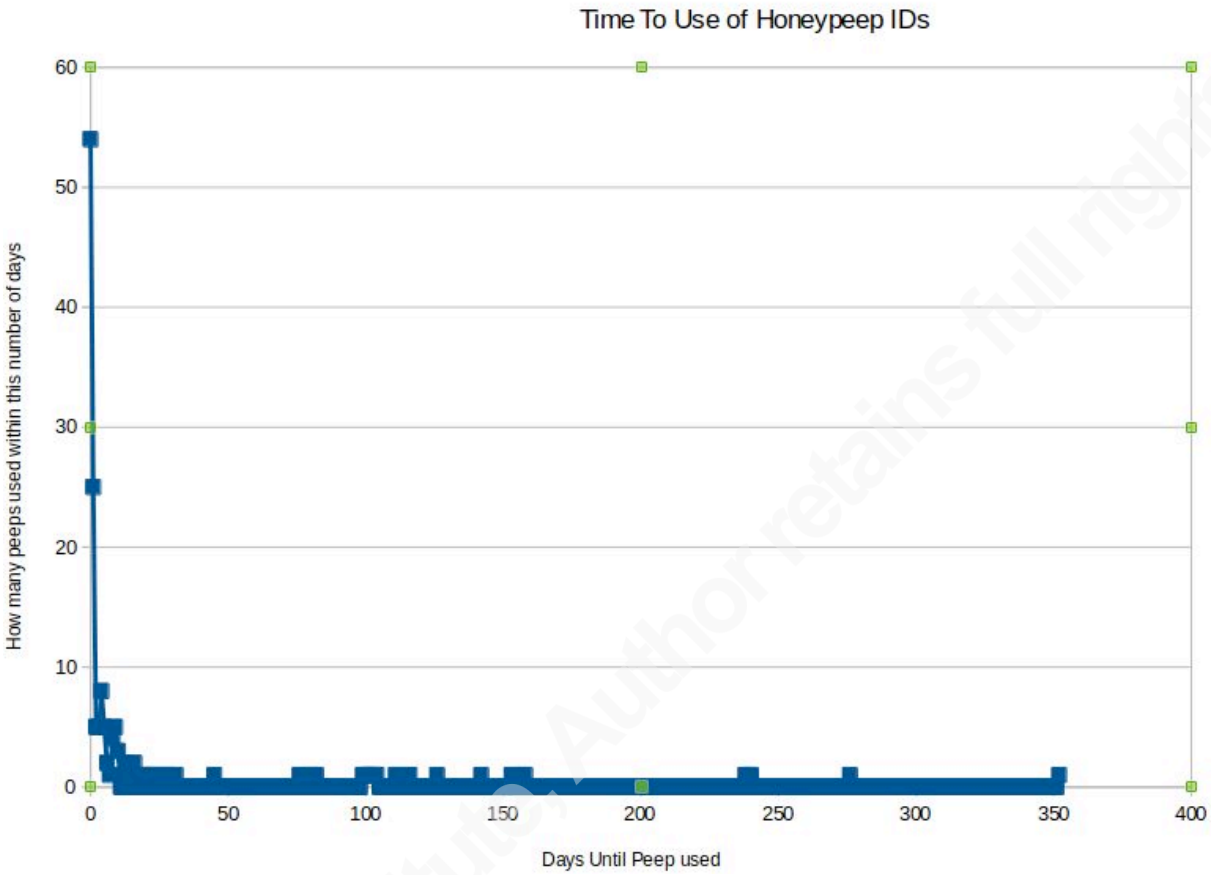


Figure 20: Response time to use of honeypeep IDs

The IPs cataloged represent a variety of use patterns—some are one-off and may come from dynamically allocated pools, or are borrowed (compromised) accounts that the phisher uses briefly. On the other hand, certain IPs appear over and over and are likely to represent a phisher's home location.

In one incident, a honeypeep salted in a form was used almost immediately from a foreign country. When it failed, it appeared twice more, from two .edu VPN addresses. Our conclusion was that they assumed we denied foreign access, but the account would work if they used the (presumably stolen) VPN accounts[2].

By collecting IP addresses used with our honeypeep project we can augment the watch list we have built from compromise events. The advantage of taking this

2 Our incident response team then notified the educational institutions of the suspected account hijacking.

action is that we can gain new IPs to watch without having a real account compromised. In a number of cases we also discovered real accounts that were being used by the phishers as soon as we were alerted to the possible attacker IP.

2.4. Other Measures and Future Considerations

Raising the awareness of this problem through user education will reduce the number of victims captured. Combined with a way for users to report phishing attempts, along with systematic incident response, an institution can stave off attacks. Our school has provided a dedicated address for people to report possible phishing attacks, and has set up an educational blog, with examples of phishing attempts directed at the university. While these examples are of known phishing, i.e., ones we have blocked on our network, our aim is to help users recognize new attempts and respond appropriately. Our incident response team blocks new attempts when reported and works to close web pages being used to phish.

Because advanced phishers have constructed pages copied from existing login forms in our domain, we've also established a monitoring process to detect web servers linking to our web content. This is another use of existing audit logs to discover and prevent phishing attacks. Such counterfeit pages are then handled as if they were a new report: blocked on our network, salted with a honeypeep test ID, and, if possible, notifying hosting providers. As always, it is necessary to determine if the pages are hosted at a reputable provider or compromised host to decide the course of notification.

With our mail system administrators, we've established a Spam Assassin ruleset that is triggered by phishing messages. Any messages matching the rules will be flagged as "spam" to warn the recipient. Our university had already offered users an optional Spam Assassin filter to tag general spam email, and once we began to see the volume of spear-phishing spam being received, we added the mandatory Spam Assassin filter tuned specifically to spear-phishing for all mail received.

That spear-phishing ruleset is continually improved, and, while generally effective, we have to acknowledge that this is a moving target—we can be surprised by new messages that don't get tagged (and then we update the rules).

Every aspect of our anti-phishing program needs to be flexible. Past performance is no guarantee of future behavior, as we've seen the phishers adapt and change over time. Also, with the growth of software as a service and cloud-based resources

(notably email services such as provided by Google and Microsoft) it may become less possible to review logs to identify misuse.

Finally, as we look at the evolving spear-phishing threat, we need to consider how to anticipate what will need to be updated and revised in the tools we use to detect and respond to the phishers. For my part, this table is a start in reflecting on how this will unfold:

Information	Source	Weakness/Risk	Future Opportunities
Authentication Events	Institutional authentication system	Anonymous, stolen access – reducing effectiveness of IP source lists	Better profiling of user behavior, increasing the ability to detect anomalous access and actions
Mail Activity indicating spamming/phished account	Local MTA infrastructure	Moving infrastructure into SaaS/cloud providers, eliminating (or reducing) log data used to detect spamming.	Use of reports from SaaS providers.
VPN activity, demonstrating compromise	Central AAA resource logging	Anonymous access, stolen accounts.	Again, better profiling of user behavior, increasing the ability to detect anomalous access and actions

Table 1: Future considerations for detecting phish.

Author: Joel Peter Anderson, joela@umn.edu

2.5. Conclusions – Information is the Key

The key to success for the phisher is ignorance on the part of the victim. The earlier quote from *How to Succeed In Business*, "big enough so that nobody knows exactly what anyone else is doing" is an apt description of the kind of ignorance that pervades many large organizations, especially universities. The advantage to the spear-phisher targeting a school is that the ever-refreshing pool of naïve victims will never be exhausted. There are enough departments and colleges within universities that many newcomers will lack knowledge to evaluate spear-phisher messages.

But information exists that can counter these attacks. With a coordinated effort all the information generated within the institutional network can be collated and discrepancies noted. History from incidents can be collected and applied to the ongoing logs. Reconnaissance through efforts like honeypeeps can expose the phishers strategy and operations.

The phishers are persistent and adaptable. They have gone from simple "please mail me your password" to rudimentary, then more complex, webforms. But it's your network, your identity, and your authentication systems. With attention to the data you already have, you can reduce the phishers' catch.

Author: Joel Peter Anderson, joela@umn.edu

3. References

Anti-Phishing Email Response (APER) group, https://groups.google.com/forum/#!forum/anti-phishing-email-reply-discuss ; web forum spun off of HIED-EMAILADMIN list.

Broome, David, "Back to School; Time to Go Phishing", February 23rd, 2011, http://labs.m86security.com/2011/02/back-to-school-time-to-go-phishing/

Dickens, Charles,"Reprinted Pieces by Charles Dickens - Free Ebook." 2006. 14 May. 2014 http://www.gutenberg.org/ebooks/872

Even, Loras, "Intrusion Detection FAQ: What is a Honeypot?", "Decoy servers or systems setup to gather information regarding an attacker or intruder into your system", https://www.sans.org/security-resources/idfaq/honeypot3.php

Everett-Church, Ray, "The Spam That Started It All - Wired." 2014. 14 May. 2014 http://archive.wired.com/politics/law/news/1999/04/19098

Fontana, John, "Password's rotten core not complexity but reuse | ZDNet." 2013. 5 Jun. 2014 http://www.zdnet.com/passwords-rotten-core-not-complexity-but-reuse-7000013019/

Goodman, J. "Spam and the ongoing battle for the inbox | February 2007 ..." 2009. http://cacm.acm.org/magazines/2007/2/5730-spam-and-the-ongoing-battle-for-the-inbox/fulltext

Hardy, G. Mark, "The Critical Security Controls: What's NAC Got to Do with IT?." 2014. 18 Aug. 2014 http://www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-what-039-s-nac-it-35115

Herley, C., "A Profitless Endeavor: Phishing as Tragedy of the Commons ..." 2008. http://research.microsoft.com/apps/pubs/?id=74159

Herley, C., "The Plight of the Targeted Attacker in a World of Scale ..." 2010. 19 May. 2014 http://research.microsoft.com/apps/pubs/?id=132068

HIED-EMAILADMIN – https://listserv.nd.edu/cgi-bin/wa?A0=HIED-EMAILADMIN, Email Administration in Higher Education mailing list.

Higbee, Aaron, "2-factor authentication wouldn't have prevented AP Twitter hack", http://phishme.com/2-factor-authentication-wouldnt-have-prevented-the-ap-twitter-hack/

Higgins, Parker, "How to Enable Two-Factor Authentication on Twitter (And Everywhere Else)" https://www.eff.org/deeplinks/2013/05/howto-two-factor-authentication-twitter-and-around-web

Author: Joel Peter Anderson, joela@umn.edu

kmov.com, "New phishing scam redirects pay checks meant for Wash U." : http://www.kmov.com/news/crime/New-phishing-scam-redirects-pay-checks-meant-for-Wash-U-employees-226387131.html

Krebs, Brian, "The Value of a Hacked Email Account", http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Lemos, Robert, "Universities fend off phishing attacks", http://www.securityfocus.com/news/11504

Mead, Shepherd. How to Succeed in Business Without Really Trying: With a New Introduction by Stanley Bing. Simon and Schuster, 2011.

Medina, Daniel and Selsky, Matt,"GULP: A Unified Logging Architecture for Authentication Data", Columbia University, Pp. 1-5 of the Proceedings of LISA '05: Nineteenth Systems Administration Conference, (San Diego, CA: USENIX Association, December, 2005). https://www.usenix.org/legacy/events/lisa05/tech/full_papers/selsky/selsky_html/index.html

Nakashima, Ellen, "Chinese hackers who breached Google gained access to sensitive data" Washington Post 20 May2013, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html

netmotionwireless.com, "Mobile Network Access control: Extending Corporate Security Policies to Mobile Devices" at the Wayback Machine (archived October 5, 2011) : https://web.archive.org/web/20111005031946/http://www.netmotionwireless.com/uploadedFiles/Resources/white_papers/NAC_WP_2010Q1.pdf

New, Jake, "Oxford Blocks Google Docs in Response to Phishing Scams ..." 2013. 26 Jul. 2014 http://chronicle.com/blogs/wiredcampus/oxford-blocks-google-docs-in-response-to-phishing-scams/42401

Phishing Scams Targeting the UMN , http://z.umn.edu/phishing

Richmond, Riva. "The RSA Hack: How They Did It - NYTimes.com." 2011. 14 May. 2014 http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it

Rosenblatt, Joel, "GULP – Grand Unified Logging Program",http://www.nysernet.org/workshops/2011/GULP.pdf

rsa.com, "Anatomy of an Attack - The RSA Blog and Podcast." 2012. 14 May. 2014 https://blogs.rsa.com/anatomy-of-an-attack/

sedward5.com, "Detecting Credential Theft Using Splunk Geographic Information,", http://www.sedward5.com/detecting-credential-theft-using-splunk-geographic-information/

Author: Joel Peter Anderson, joela@umn.edu

Schneier, Bruce, “Two-Factor Authentication: Too Little, Too Late”, Communications of the ACM, April 2005,https://www.schneier.com/essays/archives/2005/04/two-factor_authentic.html

Singh, NP. "Online Frauds in Banks with Phishing." Journal of Internet Banking & Commerce 12.2 (2007).

Snopes.com "snopes.com: Nigerian (419) Scam." 2004. 19 May. 2014 http://www.snopes.com/crime/fraud/nigeria.asp

Snyder, Joel, "NAC: What went wrong? | Network World." May 24, 2010 http://www.networkworld.com/article/2209345/security/nac--what-went-wrong-.html

"SpamAssassin: Welcome to SpamAssassin." 2004. 6 Jun. 2014 http://spamassassin.apache.org/

Thomas, Keir, "Password Reuse Is All Too Common, Research Shows ..." 2011. 5 Jun. 2014, http://www.pcworld.com/article/219303/password_use_very_common_research_shows.html

uoguelph.ca, “What are the benefits of Single Sign-On (SSO) ?”, https://www.uoguelph.ca/ccs/security/internet/single-sign-sso/benefits

Wang, D. "A Study on Evolution of Email Spam Over Fifteen Years." 2014. http://www.cc.gatech.edu/~wang6/download/dewang_2013_emailspam.pdf

Wikipedia, "Laurence Canter and Martha Siegel" 2009. 14 May. 2014 http://en.wikipedia.org/wiki/Laurence_Canter_and_Martha_Siegel

Woodhouse, Kellie, “University of Michigan warns against email scams as some direct deposit accounts are compromised” : http://www.annarbor.com/news/university-of-michigan-spear-phishing/

Author: Joel Peter Anderson, joela@umn.edu