THE PHISHING REPORT

• LEARN HOW PHISHING SCAMS NET CRIMINALS
  $5.9 BILLION A YEAR

• FIND OUT HOW BUSINESSES LIKE YOURS ARE BEING SPECIFICALLY TARGETED, & WHAT YOU CAN DO ABOUT IT
Introduction

In the first quarter of 2014:

- A security research group warned that an overseas crime group is having a high rate of success defrauding U.S. businesses of amounts ranging from $50,000 to $1 million by setting up web sites and sending emails that appear to come from vendors with relationships to these companies.

- The IRS warns that 20,000 people have reported that criminals used anonymizing voice-over-IP technology to pretend to be IRS agents in phone calls that demand back taxes or otherwise face arrest, deportation or loss of a business or driver’s license; the scam has cost victims over $1 million.

- Michigan public school officials were sent targeted emails that impersonated the finance director in a money transfer request; a $163,500 transfer was prevented due to an inquiry by district’s bank and action by alert officials in the finance office.

- 8,300 patients of Washington-based Franciscan Medical Group (FMG) had their personal information exposed to criminals who sent information requests appearing to come from FMG’s parent company; 20 employees responded to the emails.

- 1,800 patients at UC Davis may have had their personal information stolen by phishing criminals who sent emails targeted specifically at physicians at the hospital.

- An eastern European gang is using SMS text messaging to request that targets call their bank to reactivate a payment card - those who call are asked to provide their payment card and PIN number via an interactive voice response system; the scam is estimated to be worth up to $120,000 in daily ATM withdrawals.

Phishing is an approach used by criminals who pretend to be a trustworthy entity in order to persuade their victims into sharing sensitive information such as usernames, passwords, credit card details, or into downloading malware tools that can be used to steal credentials and financial information, or capture commercially sensitive data. These approaches can come via emails, SMS or other messaging tools, conversations on internet forums and social media sites, branded web sites designed to imitate a trustworthy organization, phone calls, or a combination of these approaches.

It is the 21st century version of a category of crime with a history as old as it is dishonorable - the confidence trick. Confidence tricksters will misrepresent themselves in order to gain trust, with the aim of deceiving people into sharing information or performing an action that will benefit the criminal.

Confidence tricks rely on a good understanding of psychology and the factors that motivate people. Before email became widespread, the range and influence of these scams were limited - in most cases, they occurred face-to-face and a scammer could only take advantage of a limited number of individuals in their immediate locale. The risk of detection and retribution was ever-present, so confidence tricksters had to cover their tracks well and keep moving once a scam was detected.

With today’s mass communication tools and the anonymizing abilities of technology, this is no longer the case.

Table of contents

pg. 2 Introduction
pg. 3 The Size of the Problem
pg. 4 Risk Factors & Impacts
pg. 5-6 Be Careful What You Click For: Security Tips for Managing Phishing Risks

The Shield newsletter is for...

- Business professionals and leaders with responsibility for business account management, including payroll, wire transfer and/or ACH services
- Business owners without IT support, or businesses that do not have Information Security and/or business account management policies or processes in place
- Customers of U.S. Bank and other financial institutions

Information shared in this newsletter is not intended to supersede your existing IT, account management, and/or security processes, systems or policies in your workplace, or those of your current FI. Please consult your IT support and your FI providers for more assistance.

This newsletter outlines certain practices that businesses should consider to reduce the likelihood of loss caused by online fraud and identity theft. The content does not purport to identify all existing online fraud and identity theft practices and all fraud mitigation measures that your business should consider implementing. There is no way to guarantee that any set of protective measures will eliminate loss caused by online fraud and identity theft. U.S. Bank is not responsible for losses caused by online fraud and identity theft.
According to the Microsoft Security Intelligence Report V16, between July and October 2013, emails that link to phishing sites made up more than 4% of the 85 billion spam emails detected by Microsoft’s Exchange Online Protection, a service used by tens of thousands of Microsoft enterprise customers. More than 7% of spam comes in the form of a different kind of phishing attack, where the email contains a malware-infected attachment or links to a hacked web site or file storage location that downloads malware onto the victim’s computer.

In the Evolution of Phishing Attacks report, security vendor Kaspersky Labs discovered that nearly one in nine phishing attacks their users faced came via email - for every one phishing attempt sent by email, their users faced more than eight phishing attacks via the browser pop-up ads and banners, forums and blog messages, or social media messages and status updates.

According to Symantec Corp.’s 2014 Internet Security Threat Report, although the total number of emails used per phishing campaign has decreased and the number of those targeted also decreased, but the average time of the campaign increased 3x to eight days. Symantec attribute these “low-and-slow” campaigns to spearphishing, phishing campaigns that are researched and targeted at specific companies and individuals within those companies. Personalizing phishing emails and social media messages can improve the probability of successfully fooling a target.

Google scans billions of URLs per day looking for unsafe websites and new phishing sites are detected and reported. Phishing sites are designed to imitate a legitimate web site with the intent of tricking users into typing in their username and password or sharing other private information. Typical approaches may impersonate legitimate bank web sites, online stores, or social media services.

91% increase in personalized, specifically targeted (“spearphishing”) attacks

According to Symantec Corp.’s 2014 Internet Security Threat Report, although the total number of emails used per phishing campaign has decreased and the number of those targeted also decreased, but the average time of the campaign increased 3x to eight days. Symantec attribute these “low-and-slow” campaigns to spearphishing, phishing campaigns that are researched and targeted at specific companies and individuals within those companies. Personalizing phishing emails and social media messages can improve the probability of successfully fooling a target.
Risk Factors & Their Impacts

**Hacked web site**
Malware or a phishing page can be created on someone else hacked site that is linked to in an email or social media message
- Sites like these may reveal themselves if you mouse over a suspect link and the URL that appears at the bottom of your browser or email client has little relevance to the subject matter of the email

**Phishing site**
The criminal has registered a domain and set up a page that closely imitates a legitimate branded site
- The URL may look very similar to a legitimate site, but sometimes will have subtle changes - *microsoft-online.com* or *m1crosoft.com* rather than *microsoft.com*
- A log-in page may try to extract more information than you are used to seeing when logging on to the regular site

**Bogus attachment**
The message comes with an attachment that may be a zipped file or a document that seems to be business-relevant
- It may have malware attached; many spearphishing attacks use this approach
- It may be a form designed to gather more information from you or your employees
- Word, Excel, PDF and zip files are high risk; be cautious unless you expected the attachment

**Pop-up warnings**
Be suspicious of warnings that appear, asking you to install media players, document viewers and security updates
- These attacks can often lead to ransomware installs, where your files are locked until you pay a fee to the criminals
- Only download software updates direct from the vendor

**Social media**
Phishing attacks either coming from a hacked social media account or attempting to steal social media credentials have surpassed email attacks
- 30% of all phishing web sites use faked social media log-in pages designed to steal social media credentials
- Phishing criminals use information available on employee social media pages to target spearphishing attacks

**Spearphishing**
Aimed at individuals or groups, using data gathered from social media, web searches, or previous phishing; may appear to come from a trusted source and could feature business-relevant or personal data
- 30% of spearphishing targets small-to-medium businesses (Symantec)
- 67% of cyber-espionage begins with phishing, typically spearphishing (Verizon)

**Phishing impacts**
Falling for a phishing attack can lead to:
- Theft of passwords and log-in information, which can mean:
  - Financial loss in the form of stolen banking credentials, or other business account information
  - Identity theft that can harm credit ratings
- Credential thefts that allow criminals to take over your social media accounts, email accounts, or even your company web site, which phishers may use to:
  - Contact your business contacts using your name to send spam or malware
  - Stealthily explore deeper into your network, possibly turning a foothold into a full-scale breach
  - Access any shared resources you have with clients to find a way onto their networks
- Malware installs to exploit your network or other accounts, or to use your social media or web resources to infect others with malware, leading to:
  - Financial loss, records loss, unauthorized access to retail and financial accounts
  - Lost traffic to your web site if it is blacklisted by Google and other search engines
  - Lost sales and contracts, and damage to your reputation

The cost of cleaning up can be extremely high. In March, 2013, the U.S. House Small Business Subcommittee on Health and Technology hearing Thursday on the topic of “Protecting Small Businesses Against Emerging and Complex Cyber-Attacks” heard that nearly 60% of small businesses will shutter within half a year after being victimized by cybercrime.
Be Careful What You Click For
Security tips for managing phishing risks

Unfortunately, there’s no one preventative solution that will work without fail in all cases. The most effective security is layered security, where different approaches work together to minimize the chance of a successful phish. However, should one get through, additional security layers reinforce each other for effective failover, where the ideal end result is improved detection time and minimized impact to you, your business, and your customers:

- **Prevention through user security awareness**: Aware users are less likely to be the victims of phishing attacks.
- **Prevention through software**: Up-to-date, effective and thoroughly patched software tools are more likely to detect potential threats or be less vulnerable to the malware software exploits that can result from incautious clicks.
- **Detection & impact limitation**: Knowing what to look for, ensuring all users are able to identify and report possible phishes, and putting tools in place such as multi-factor authentication and account control (see the 1st edition of the Shield, “Malware, It’s a Bear for Business”) can make significant contributions in limiting the damage resulting from a successful phish.

Understand the psychology behind a phishing attack

- When the content of a message featuring a link or attachment leaves you startled, fearful, indignant, confused or intrigued, be careful. Another warning is any pressure applied on you to take immediate action - criminals want you to react emotionally when thinking twice is more appropriate.

- If an offer, deal or story seems too good to be true, it probably is.

- Just because someone emailing or calling you seems to know a lot about you or has mutual friends, acquaintances or colleagues in common, that doesn’t automatically make them more trustworthy - spearphishers count on our tendency to be more trusting of extended network contacts.

- When a communication appears to come from a company or service that you use, it could still be a phishing attack - criminals count on complacency bred by familiarity - it’s habit for most people to just open that social media friend request, or that package tracking link from our email (see figure 1). However, it doesn’t take much more time to type the site address into a browser and view the information firsthand instead of clicking a link or attachment. You can copy the tracking number from the concerning message and paste it onto a handy tracking widget on the main page of their site.

- Scammers can fool us by pretending to be someone in authority - an FBI agent, a lawyer, a technical specialist from Microsoft, or even someone in your own IT organization. Don’t let yourself be pushed into action without doing independent checking.

- We are more likely to trust a communication from someone we know, and phishing criminals take advantage of this. If they are able to hack into a social media or email account, they will send phishing material via email, messages, or in-status updates that will appear to come from the person whose account they hacked - if the message seems out of character, then beware.

**Content warnings**

- If you’re being contacted about existing services and accounts at companies whose services you don’t use or in regards to a transaction, invoice or delivery that you never requested, that’s a clear danger sign.

---

**Figure 1**: Example email phish - note the mouseover URL difference, the spelling issues, and the email address discrepancy.
• When you spot a warning sign in a message, don’t click on any links, interact with attachments in any way, or reply to the sender directly - use a search engine to track down the sending organization’s contact info, then pick up the phone or email to confirm with the sender or a suitable representative that this email came from them. Don’t just hit “reply” - if it happens that someone else’s email or social media account was hacked, then the person you reply to may be the hacker.

• Phishing emails that imitate real brands are sometimes riddled with grammar and spelling errors that you would not expect to see from the actual organization (see figure 1); these mistakes are a reliable warning sign but their absence doesn’t mean an email is legitimate - spearphishers may avoid making these mistakes in their communications to make them as believable as possible.

• Use the mouseover trick (see figure 1) and hover your cursor over an embedded link to see where it really goes (a feature available with most browser and email clients). If the link text seems to be for a download of your preferred tax preparation software but your mouseover reveals that the link is hosted on a BMX biking web site, that’s a red flag. However, know that phishers will sometimes go to great lengths to hide that they’re using a hacked site, so even if the link looks legitimate, it doesn’t mean that it actually is. It’s simplest and most effective to just look up the originating company’s web site and find the information yourself.

• Link shortening services are convenient for masking an extra-long web address in favor of something shorter and more memorable, but they’re also great for hiding a phishing site destination (bit.ly is particularly popular for phishing campaigns). Avoid clicking on shortened links until you’ve first checked it out with the sender, or until you’ve used a preview or plug-in tool to expand its destination.

• Make sure you have a secure transaction session in place before submitting personal or financial information to a web site - check the browser address bar to make sure the address begins with “https”, and look for a padlock icon on the browser status bar - be aware that although this does not absolutely guarantee security, the absence of either means your transaction is definitely insecure and likely indicates that something is not right.

Attachments & downloads
• Assume all links and attachments sent to you via email or social media are potentially hostile, even when you know the sender - unless you have reason to expect them. Double-check when in doubt.

• Generally avoid downloading any software or files from unknown sources; stick to mainstream sites.

• Any window that pops up to warn you about security while advising a software update, or suggests an update or software install when you are surfing the web or opening an attachment is suspect - never accept the install from the pop-up - instead, go to the software vendor’s web site and do the install manually.

• Avoid clicking anywhere on a pop-up window warning you about malware or antivirus - even to close it. PC users can use Alt F4, CTRL W, or the task manager to close the browser instance instead.

For more tips:
https://www.usbank.com/security
http://www.usbankconnect.com/searchall/technology

Do you manage your own IT?

Microsoft OS
• Ensure PCs are running Windows 7 or later - the more recent the OS, the more advanced its security features
• Make sure that Windows is automatically installing critical patches - Click the Start button, click All Programs, and then click Windows Update to check
• Read and bookmark the Microsoft Security Site1
• Download and run the Microsoft Safety Scanner2 every few months or so to sweep for malware that could have evaded your antivirus
• Read reviews4 to choose a fully-featured and high-performing antivirus software tool (one with anti-phishing features); make sure it is kept up-to-date
• Make sure you have the latest versions of Internet Explorer, Firefox or Chrome - current browsers have built in anti-phishing protection
• Ensure that all software is patched and up-to-date: particularly Oracle Java and Adobe tools like Flash and PDF readers
• Internet Explorer users should enable SmartScreen Filters6 for additional anti-phishing and malware protection

Apple OS
Although not subject to the same volumes of malware that PC users face, Apple users are specifically singled out in branded phishing campaigns and are just as vulnerable to credential and personal data phishing that rely on user input rather than malware. Learning to avoid phishing is critical.

Trusteer Rapport
US Bank has partnered with Trusteer to offer the Rapport anti-fraud software to our SinglePoint customers for free. This powerful tool provides protection from financial malware, zero day threats, phishing attempts, and will complement your existing security profile to produce a stronger, layered web of defense. Rapport is available for download via the SinglePoint splash screen, footer links, or by accessing Trusteer directly6.

Report cybercrime
If you are the victim of a successful phishing attack, report it right away. Where may depend on the crime, so bookmark the Department of Justice’s contact page7 to find the right local and/or federal law-enforcement group.

You may also need to report to your financial institutions, vendors and customers, and state regulatory bodies. Experian’s Data Breach Response Guide6 is a comprehensive tool for businesses of all sizes.

1 http://www.microsoft.com/security/
2 http://www.microsoft.com/security/scanner/
3 http://www.av-comparatives.org/
4 http://www.av-test.org
6 http://www.trusteer.com/landing-page/usbank-business
7 http://www.justice.gov/criminal/cybercrime/reporting.html

U.S. Bank SinglePoint is a registered trademark of U.S. Bank National Association.
U.S. Bank makes no warranty of any kind as to the effectiveness of the Trusteer Rapport software. U.S. Bank is not responsible for and does not guarantee the products, services or performance of third parties.