2018 Public-Private Analytic Exchange Program

Vulnerabilities of Healthcare Information Technology Systems

Phishing: Don’t Be Fooled!

PWNED

01011001 01001111 01010101 00100000 01001000 01000001 01010110 01000101 00100000 01000010 01000101 01000101 01001110 00100000 01010000 01010111 01001110 01000101 01000100 00100001
# Table of Contents

Acknowledgement ............................................................................................................. ii
Executive Summary ............................................................................................................. 1
Level Setting and Cyber Threat Landscape ........................................................................ 2
An Introduction to Phishing ................................................................................................. 2
Psychology of Phishing ....................................................................................................... 5
Anatomy of a Phishing Attack ............................................................................................... 7
New Phishing Techniques .................................................................................................... 8
Mitigating Phishing Attempts ............................................................................................... 9
Conclusion and Recommendations ..................................................................................... 12
Appendix A: Sample Phishing Emails Received by Healthcare Organizations .................. 13
Appendix B: Where to Report Phishing ................................................................................ 25
Acknowledgement

We acknowledge and thank the federal government agencies and companies that supported the development of this paper. We also thank the Office of the Director of National Intelligence (ODNI) and the U.S. Department of Homeland Security (DHS) for the opportunity to have participated in the 2018 Public-Private Analytic Exchange Program (AEP).

People and Organizations Consulted

We are grateful to the individuals and companies that provided their time to advise, answer questions, and assist in developing the information in this report:

- Axel Wirth, Distinguished Technical Architect, Healthcare Practice, Symantec Corporation
- Dermot Harnett, Director of Development, Security Technology and Response (STAR), Symantec Corporation
- Vikram Thakur, Technical Director, Security Technology and Response (STAR), Symantec Corporation
- Jason Hawley, Director of Information Services and Security
- Kevin Johnson, Secure Ideas
- Bayardo Alvarez
- Paul Scheib, Senior IT Director, Boston Children’s Hospital
- Jigar Kadakia, Chief Information Security and Privacy Officer, Partners HealthCare
- Debbie Mikelis, OTR/L, FHIMSS, Information Security Program Manager, Partners HealthCare
- Martin McKeay, Akamai Technologies
- Josh Corman, I am the Cavalry
- Julian M. Goldman, MD, Director, Medical Device Interoperability & Cybersecurity Program, Massachusetts General Hospital; Medical Director, Partners HealthCare Biomedical Engineering; Anesthesiologist, Massachusetts General Hospital
- Al Roeder, HCCIC, OCIO, U.S. Department of Health and Human Services
- Kevin Allen Dorsey, Deputy CISO, Centers for Medicare & Medicaid Services, U.S. Department of Health and Human Services
- Stephen Curren, Director, Division of Resilience, Office of Emergency Management, Assistant Secretary for Preparedness and Response, U.S. Department of Health and Human Services
- Nick Heesters, Office for Civil Rights, U.S. Department of Health and Human Services

Public/Private Team Members

- Hany Wassef, Meritor
- Bruce de'Medici, Grey Oar
- Lee Kim, JD, CISSP, CIPP/US, Healthcare Information and Management Systems Society
- Sandra Hemmes, Humana
- Chris Letterman, Wostmann & Associates
- Kevin Littlefield, MITRE Corporation
- G. Squire, National Security Agency
- C. Myers, National Security Agency
- S. Dixon, Central Intelligence Agency
- Torrey Kingcade, U.S. Department of Justice
- Benjamin Amsterdam, U.S. Department of Defense
- William Pachucki, CISSP, U.S. Department of Health and Human Services
Executive Summary

Phishing is a significant threat to everyone, including healthcare organizations. Many significant security incidents originate with a successful phishing attempt. Inboxes are no longer clogged with “junk mail”, but rather with phishing emails designed to elicit sensitive information, deploy malware, or achieve another end.

Malicious actors know that phishing is a highly effective means to penetrate an organization and its people. The phishing threat is constantly evolving. Thus, the asymmetric threat is real. Defense capabilities often pale in comparison to offensive capabilities in the healthcare and public health (“HPH”) sector. Human and technical controls either do not evolve or tend to evolve slowly in many healthcare organizations.

But, there are some small, medium, and large healthcare organizations that have sophisticated cybersecurity programs in place. These organizations practice defense in depth and have successfully integrated their people, processes, and technology to work as one unified whole. While achieving one-hundred percent security is generally not possible, the advantage of having a robust cybersecurity program is that the blocking and tackling occur much more quickly and efficiently.

Through a series of virtual and in person interviews, literature reviews, and other engagement, this educational paper provides a holistic perspective on phishing: what it is, how effective it is, the impact, how phishing occurs, what some new phishing techniques are, and how to mitigate the phishing threat.
Level Setting and Cyber Threat Landscape

Traditionally, many healthcare organizations approached healthcare cybersecurity from a compliance-based perspective. The top concern was having a data breach. But, a significant turning point was in August 2014 when a major hospital system made a public announcement to the media that it had been the victim of a significant cyber-attack and 4.5 million patient records had been breached.\(^1\) Since then, cyber-attacks and other compromises have grown in sophistication, volume, and frequency. Further, while data breaches continue to occur, healthcare organizations must now worry about compromises involving the integrity and availability of data (e.g., ransomware, denial of service, insider threat, etc.).

While many healthcare organizations are improving the state of their cybersecurity programs, such improvements may not be enough to sufficiently stay ahead of the threats. The threats are numerous and complex. Attackers look for open doors or windows into organizations. An efficient and effective way into healthcare organizations is through social engineering (i.e., exploiting the human factor).\(^2\) Phishing is a pervasive threat for all organizations. Healthcare organizations, too, are vulnerable.\(^3\)

An Introduction to Phishing

*Phishing* is a social engineering tactic that is used to persuade individuals to provide sensitive information and/or take action through seemingly trustworthy communications.\(^4\) The three major categories of phishing are as follows: (1) general phishing, (2) spear-phishing, and (3) whaling. Malicious actors employ phishing techniques for a variety of reasons, including identity theft, access to proprietary information, transmission of malicious software to include ransomware, unauthorized remote access, and initiation of unauthorized financial transactions.

The most common form of phishing is the phishing email. Phishing emails may attempt to appeal to a recipient’s fear, duty, obligation, curiosity, or greed.\(^5\) Early forms of phishing emails (i.e., general phishing) did not target specific individuals. Such phishing emails are still prevalent today and contain...

---

hallmarks such as poor grammar, spelling, and, often, “too good to be true” claims.6,7 A phishing email may appear to originate from a well-known company, agency, university, or individual.8,9 Examples of general phishing, spear-phishing, and whaling emails may be found in Appendix A.

A general phishing email may elicit sensitive information or money from the recipient and/or contain malicious hyperlinks, attachments, and code.10,11 Thus, opening an email message (which may have a malicious script, image, and/or video) or, an attachment, and/or clicking on a malicious link may lead to compromise. Because general phishing is an untargeted form of attack, malicious actors typically cast a wide net with the hope that some recipients take the bait.

In contrast, spear-phishing is a targeted phishing attack.12,13 Spear-phishing is a popular infection vector for malicious actors.14 Spear-phishing messages are tailored to the target recipient (e.g., individual or groups within an organization).15 There is a plethora of information available online about companies, their employees and contractors, current and past projects, policies and procedures, and their vendors and business associates. Spear-phishing messages may be particularly convincing when they contain “insider information” relevant to the targeted organization or individual. In addition, spear-phishing has

---

been made more effective through the use of stolen vendor credentials.\textsuperscript{16} Thus, spear-phishing has been used to target healthcare organizations, either directly or indirectly (such as through vendors).\textsuperscript{17}

Similarly, whaling is defined as a targeted phishing attack that is aimed at wealthy, powerful, or prominent individuals (e.g., C-suite executives such as chief financial officers and chief executive officers, politicians, and celebrities).\textsuperscript{18,19,20} But, others use the term “whaling” to mean an attack that involves malicious actors masquerading as such individuals.\textsuperscript{21} As an example, a malicious actor may masquerade as a hospital’s chief financial officer (“CFO”) and trick the recipient into divulging bank account information, employee information, corporate financial information, and/or transferring funds to an account that is controlled by the actor.\textsuperscript{22}

According to recent studies, the initial point of compromise for significant security incidents is generally by way of phishing.\textsuperscript{23,24} These security incidents may adversely affect the confidentiality, integrity, and/or availability of information (e.g., protected health information, personally identifiable information, employee information, intellectual property, and other sensitive information). But, the greatest risk to healthcare organizations is patient safety. Threats to patient safety may exist as a result of any compromise to the confidentiality, integrity, and/or availability of information.\textsuperscript{25} Thus, something seemingly as simple as phishing needs to be addressed, as a successful attack may open the door to patient safety issues.

\textsuperscript{16} This type of attack has been prevalent since at least 2014. A major cyber-attack affected a well-known retailer in December 2013.
Anyone can be a victim of a phishing attack, including end users and information technology professionals.\textsuperscript{26} People who do not consider themselves to be trusting by nature may be vulnerable when presented with a convincing story.\textsuperscript{27}

Factors which may make people more susceptible include using a mobile device (as it may be more difficult to scrutinize links and content of messages),\textsuperscript{28} accessing email outside of regular business hours, and being mentally fatigued (e.g., early morning, late in the day, etc.).\textsuperscript{29} But, malicious links may be obfuscated as well. Malicious actors use shortened uniform resource locator ("URL") services to mask their (malicious) links in emails, text messages,\textsuperscript{30} and social media messages.\textsuperscript{31,32}

**Psychology of Phishing**

Phishing attacks may be used by malicious actors to defeat security controls by exploiting weaknesses in decision making and human behavior. Such attacks often rely on a combination of tactics to influence decision making such as authority, time pressure, and tone, as people tend to comply with requests from authority figures. This is why phishing emails that claim to be from a trusted source with a corporate logo or name appear to have legitimacy and credibility. Further, clues to the fraudulent nature of phishing scams often fall below the threshold of the average recipient.\textsuperscript{33}

Phishing messages often contain an element of urgency and, thus, time pressure. The tone of these messages frequently involves a combination of persuasive and polite statements to also influence decision making. Such messages may also prey on a user’s fear of something, such as an account restriction or leverage current events, or these messages may seek to psychologically manipulate or exploit the emotions of the victim.\textsuperscript{34}

\textsuperscript{26} See Alison DeNisco Rayome, *Report: Phishing Attacks on the Rise, Executives and IT Workers Most Likely to Fall Victim*, available at https://www.techrepublic.com/article/report-phishing-attacks-on-the-rise-executives-and-it-workers-most-likely-to-fall-victim/. “Entry-level employees—commonly blamed for cyber breaches—are not the only ones at fault, the report found: 34% of executives/owners and 25% of IT workers themselves report being victims of a phishing email, more often than any group of office workers.” Id.


\textsuperscript{30} This is called SMiShing or smishing. See, e.g., Marc Saltzman, ‘Smishing’ Scams Target Your Text Messages, Here’s How to Avoid Them, available at https://www.usatoday.com/story/tech/columnist/saltzman/2017/07/03/delete-suspicious-text-messages-on-your-smartphone/439647001/.


\textsuperscript{32} Cf., *Shady URL*, available at http://www.shadyurl.com/. In contrast, this service makes URLs seem shady.


In the case of spear-phishing, such messages may appear quite convincing by leveraging insider knowledge about job functions, work relationships, current projects, etc.\(^{35}\)

There are some users, however, that tend to have certain personality traits and characteristics that make them more susceptible to phishing.\(^{36}\) For example, users who have a strong commitment to their organization and exhibit agreeableness may have a greater degree of susceptibility. But, well-designed security awareness training and education can benefit all groups and demographics of people to reduce the number of victims falling prey to phishing attacks.\(^{37}\)

**Most Clicked General Email Subject Lines Globally for Q1 2018.**

1. A Delivery Attempt Was Made - 21%
2. Change of Password Required Immediately - 20%
3. W-2 - 13%
4. Company Policy Update for Fraternization - 10%
5. UPS Label Delivery 1ZBE3112TNY00015011 - 10%
6. Revised Vacation and Time Policy - 8%
7. Staff Review 2017 - 7%
8. Urgent Press Release to All Staff - 5%
9. Deactivation of (email) in Process - 4%
10. Please Read: Important from HR - 2%

However, even the most sophisticated users have been fooled by some visual deception tricks used in phishing. In one study, good phishing websites fooled ninety percent of the participants. For example, users may be fooled by “typejacking” attacks which substitute letters (e.g., www.paypa1.com) or other lookalike characters (such as homographs, also referred to as homoglyphs). In another example, an image of a legitimate hyperlink leading to a rogue link may fool users. Yet another example of a technique is to place an illegitimate browser window on top of, or next to, a legitimate window, thereby tricking users into mistakenly believing that both windows are from the same source.\(^{38}\)

---


Anatomy of a Phishing Attack

There are generally six steps involved in a phishing attack:\(^{39}\)

1. **Identify the target.** The malicious actor determines who or what to target and how to obtain the email addresses. The malicious actor may decide to do a mass email to a large number of email addresses (i.e., general phishing), or the target may be specific (i.e., spear-phishing or whaling). But, before the malicious actor needs to collect the email addresses of his or her intended victims. Email addresses may be harvested from the Internet.\(^ {40}\) Email address lists may also be purchased from third parties. Email addresses may also be generated via a dictionary attack.\(^ {41}\)

2. **Craft the message.** The malicious actor crafts the message with content that is designed to make the recipient take some action, such as open a message, open an attachment, click on malicious link(s), and/or respond to a message. If the malicious actor wants to conduct a general phishing attack, then the message crafted by the actor is one size fits all. However, in the case of a spear-phishing or whaling attack, the message is customized for the target.\(^ {42}\) The malicious actor may also generate the malicious payload to accompany the crafted message.\(^ {43}\) Further, the malicious actor may clone a legitimate website to make a phishing website that he or she controls.\(^ {44}\)

3. **Deliver the message.** The malicious actor sends the message to the target(s), typically with a spoofed email address for the sender of the message.\(^ {45}\)

4. **Deception.** If the phishing attack is successful, the recipient of the message is deceived into taking the intended action or providing the desired information.

5. **Action by recipient.** The recipient performs the intended action.

6. **Disclosure.** The recipient discloses the requested information (to the extent that the phishing message requests certain information).

7. **Action by malicious actor.** The malicious actor uses the collected information for his or her end. The information may benefit the malicious actor financially or in other ways.

---


\(^ {41}\) A dictionary attack with a list of usernames may be used to guess the email addresses for a domain. See also FTC, *Candid Answers to CAN-SPAM Questions*, available at https://www.ftc.gov/news-events/blogs/business-blog/2015/08/candid-answers-can-spam-questions. The FTC notes that email lists (for purchase) may have been put together using illegal means like email address harvesting or dictionary attacks.


\(^ {43}\) The malicious payload may be generated using the Social-Engineer Toolkit ("SET"), Metasploit, MSFvenom, and other tools.

\(^ {44}\) Tools for cloning websites include Grab-a-Site, HTTrack and SET.

\(^ {45}\) The message(s) may be sent using tools such as SET.
New Phishing Techniques

Hijacking of email threads with a malicious actor masquerading as a trusted colleague, friend, or family member is a new technique used for phishing attacks. This can happen, for example, to two chief information security officers (“CISOs”) at different healthcare organizations who are having a conversation via email. The malicious actor may pose as one of these CISOs, tricking the other CISO into opening a malicious attachment.

Typejacking and/or homograph attacks may also be used to fool the recipient of a phishing message. Specifically, the sender’s domain name may look like a well-known or trusted domain name, but it actually is a “lookalike” domain name. (An example of a “typejacking” domain name is “examp1e.com” instead of “example.com.” An example of a homograph domain name is “dish.com” instead of “dizh.com.”) Specifically, a malicious actor may leverage the similarities of character scripts to create and register phony domain names that look like a trusted domain name. Thus, a phishing website could be created using the phony domain name to fool users and lure them into visiting. Yet another phishing technique involves dynamic data exchange (“DDE”) attacks using emails and calendar invites that have been formatted in rich text format (“RTF”).

Artificial intelligence may also be used to conduct (or simulate) spear-phishing attacks. For example, researchers have devised a fully automated spear-phishing system that creates tailored tweets based on a user’s interests, achieving a high click rate for links that could be malicious. Yet other researchers have devised an artificial intelligence system for automated spear-phishing which includes automatic construction and communication of a spear-phishing message that is tailored to the victim using information that is unique to that individual.

Situational awareness, security awareness training, and defense in depth are key strategies to thwart phishing attempts. The phishing threat is always evolving and so should human and technical controls. It is predicted that spear-phishing attacks will increase with the malicious use of artificial intelligence.

---


Mitigating Phishing Attempts

There are steps that healthcare organizations may take to mitigate the phishing threat. Healthcare organizations must maintain an awareness of the current phishing strategies and ensure that their security policies, security solutions, and controls effectively mitigate such threats as they evolve. It is equally essential to make sure that workforce members, contractors, and vendors understand the types of attacks that they may encounter, the risks, and how to appropriately address them.

The following is a non-exhaustive list of security awareness tips for users:

- **Identifying the potential phish.**
  - Check whether the suspected phishing message contains a generic subject and greeting.
  - Look for mistakes in the message (e.g., spelling, grammar, facts, etc.).
  - Watch out for odd looking characters, including in the message, links, and elsewhere.
  - Carefully scrutinize messages that require an urgent response or action.
  - Be cautious of messages that ask for personal, confidential, sensitive, proprietary, employee, and/or patient information (including usernames, passwords, social security numbers, medical record numbers, diagnoses, billing information, etc.).
  - Be cautious of messages that address you with the wrong name.
  - Do not click on shortened links. Consider expanding them first to reveal the actual URL.
  - Check to see if the text of the link matches the actual embedded link before clicking.
  - Trust your instincts. If the message seems suspicious or odd, err on the side of caution.

- **Checking for phish.**
  - Consider contacting the sender via an out-of-band communication channel (e.g., telephone call or otherwise) to verify the content of the communication (especially if this is someone you know or do business with).

- **Reporting the phish.**
  - Forward the suspected phishing message as an attachment to your organization’s point of contact or follow established procedures, as appropriate.
    - Let your point of contact also know of any relevant communications.

- **Raising the phishing IQ.**
  - Do participate in security awareness training initiatives.
  - Engage in security awareness initiatives such as Data Privacy Day, National Cyber Security Awareness Month, and Stay Safe Online.
  - Ask questions, learn, and engage with others about phishing.

---


The following is a non-exhaustive list of enterprise-wide tips for healthcare organizations:

- Implement basic security controls:
  - Conduct accurate and thorough risk assessments.
  - Securely configure computing equipment (e.g., anti-virus software, firewalls, etc.).
  - Deploy access controls for health IT and electronic health information.
  - Encrypt electronic health information.
  - Conduct regular backups of electronic health information.

- Implement advanced security controls:
  - Apply the principle of least privilege for all users.
  - Regularly conduct user privilege reviews.
  - Provision and de-provision accounts in a timely manner.
  - Have a robust patch management program.
  - Segment your networks.
  - Deploy multi-factor authentication.
  - Utilize email and web security gateways.
  - Configure Domain Name System (“DNS”) security filters.

---


56 See, e.g., Indiana University, About the Principle of Least Privilege, available at https://kb.iu.edu/d/amsv.


59 See Terry Zink, VB2014 Paper: Using DMARC to Improve Your Email Reputation, available at https://www.virusbulletin.com/virusbulletin/2014/11/paper-using-dmarc-improve-your-email-reputation (advantages and limitations of SPF, DKIM, and DMARC). SPF is dependent upon the global domain name system (“DNS”) to function. An organization configures the SPF record(s) in its DNS nameserver(s) and specifically identifies, by IP address, the system(s) authorized to send mail for the organization’s domain. This helps to safeguard against another entity or individual trying to send email messages from the organization’s domain. In essence, SPF helps to identify whether an email has originated from an authorized source. (The “answer” from the global DNS system in regard to the IP address associated with SPF record(s) may not match the IP address of a “forged” message, which purports to originate from the organization’s domain.)

DKIM is also dependent upon global DNS and uses generated keys to cryptographically sign an email message. DKIM verifies the source and contents of message to ensure integrity of the message. An organization creates a public and private key. The public key is stored in its DNS nameserver(s). In the case of an authorized sender (with the private key), DKIM creates a digital signature that is derived from the message contents and encrypted with the private key using public key encryption. When a recipient receives a DKIM signed email, the organization’s
• Implement anti-phishing controls
  o Use anti-spoofing controls and filter incoming messages.
  o Reduce the digital footprint of the organization and its users.
  o Tag external emails for emails originating from the outside (e.g., “EXTERNAL” and/or notice “CAUTION – This is an external email. Be careful when opening any attachments”). 60,61
  o Educate users about how to spot a phish and how to handle it.
    ▪ Frequent security awareness education is important.
      • Educate staff on anti-phishing strategies.
    ▪ See something, say something – report suspicious emails and messages to the information technology (IT) help desk, security office, or appropriate point of contact. 62
  o Alert users about ongoing phishing campaigns 63
  o Develop and analyze metrics re: anti-phishing controls.

---

public key is retrieved from the DNS nameserver(s). The public and private keys are then evaluated to determine if they match (i.e., a complementary pair). In the case of a match, the DKIM signed email is authentic. Thus, a malicious actor cannot “spoof” the email message in the absence of having the sender’s actual private key.

DMARC is also dependent upon global DNS and requires the publishing of a DMARC record to the organization’s nameserver(s). An organization that receives an incoming email message will validate an incoming email message with SPF or DKIM (as explained above). The sender’s domain name record will be queried for the DMARC DNS record. Depending upon the option flag setting in the DMARC DNS record, the email will be: (1) allowed for delivery, (2) allowed for delivery, but marked as quarantine, or (3) rejected. (Note: This depends upon the sender’s DMARC DNS record configuration.)

A weakness of DMARC is that it does not catch the instance in which the malicious actor changes the domain to make it look like the target domain (e.g., @paypa1.com). See id. (homoglyph attacks, also referred to as homograph attacks). But, organizations can help prevent this by purchasing domain names that sound or look similar to their own and then publishing SPF and DMARC records for those domains, indicating that they send no email. However, it may be impossible to register all potential lookalike and similar sounding domain names.


61 But, also educate users on the insider threat (negligent and malicious). Phishing emails often do originate from outside sources, but they can also originate from inside the organization (by a malicious insider).

62 Report the phish, as appropriate, including and especially to the points and contact within your organization. Please also refer to Appendix B in this paper.

63 Educate users about phishing campaigns that are happening currently within your organization, sector, and/or other sectors. See, e.g., University of Georgia Enterprise Information Technology Services, Fresh Phish, available at https://eits.uga.edu/access_and_security/infosec/fresh_phish/.
• What to do if phishing is suspected:
  o Respond quickly to any phishing incidents that occur.
  o Report the phish:
    ▪ Users should immediately report the phish to their organization.\textsuperscript{64}
    ▪ Consider reporting the phish to others (Appendix B).
  o Identify recipients and possible infected systems:
    ▪ Search email server logs for applicable sender, subject, and attachments.
    ▪ Search applicable web proxy, DNS, firewall or IDS logs for activity resulting from a malicious link being clicked.
    ▪ Use threat intelligence sources to search applicable web proxy, DNS, firewall or IDS logs for activity to any associated command and control ("C2") domains or IP addresses associated with the malware.
    ▪ Review anti-virus ("AV") logs for alerts associated with the malware. AV products should be configured to be in quarantine mode. The absence of AV alerts or a clean scan does not necessarily mean that a system is not infected.\textsuperscript{65}
    ▪ Scan systems for host-level indicators of the related malware with Yara rules.\textsuperscript{66}
  o For systems that may be infected:
    ▪ Capture live memory of potentially infected systems for analysis.
    ▪ Take forensic images of potentially infected systems for analysis.
    ▪ Isolate systems (e.g., with a virtual local area network (VLAN) segment).

Conclusion and Recommendations
Phishing will undoubtedly continue to be a significant threat in the future. With greater situational awareness and knowledge about attack techniques and methods, healthcare and public health sector stakeholders can become better defenders.

We encourage you to keep up with your situational awareness regarding the threats that are out there, share this information with colleagues, and collaboratively develop solutions. After all, patient safety should not be a choice. Robust cybersecurity is an imperative to protect our patients, information, assets, infrastructure, and our nation.\textsuperscript{67}

Disclaimer Statement:
“This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the U.S. Government or the Public-Private Analytic Exchange Program participants, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.”


\textsuperscript{65} In other words, be cognizant of anti-virus evasion techniques and tools. See, e.g., FireEye, \textit{AntiVirus Evasion Reconstructed—Veil 3.0}, available at https://www.fireeye.com/blog/threat-research/2017/03/_antivirus_evasionr.html and Infosec Institute, \textit{Antivirus Evasion Tools}, available at https://resources.infosecinstitute.com/antivirus-evasion-tools/.


Appendix A: Sample Phishing Emails Received by Healthcare Organizations

General phishing emails

![Phishing Email 1]

![Phishing Email 2]
General phishing emails

STOP & THINK...This is an external email! Please only open attachments and links you know to be safe!

Hello,

This is a reminder that Casey Smith shared with you document called "Payment Invoice 386283611" and left you this message:

"Please let me know if you have any questions about the invoice 386283611. ... Thank you in advance for your prompt payment." Casey

View file

Contact

Have questions or concerns about Dropbox, our Services and privacy? Contact us at privacy@dropbox.com.
General phishing emails

Greetings

Please see the bill in attachment.

Word doc Access Credentials: oEhhz

Thanks
Heath, Coby V.
Facilisis Foundation

Hello friend,
I'm a German national, but live and work in the Kingdom of Cambodia as a bank manager, i have a very important business proposal that will benefit both of us greatly if you indicate your interest in this transaction. Please contact me immediately you receive this message to proceed.

Yours sincerely,

Ole Holsemeyer.
General phishing emails

Please

To: snnooww_white@yahoo.co.jp on behalf of Zita Blanc <zittablanc@outlook.fr>

Subject: Good day,

My name is Zita Blanc, 18 years old, the only daughter to my late parent Mr. Mrs. Blanc. I am contacting you with tears because I need you to stand as my guardian in the management of a sum that my late father left for me before he died. Please I am ever ready to offer you 20% for your help. 10% will be donated to the orphans like me to help the poor, then you will help me invest the balance for me in your country. Please take me like your daughter or your sister and I pray before contact you please.

Attached here are my personal photos, evidence of deposit of the fund, my international passport and my late father’s documentation and origin of his life. I am sending all these for you to have confidence that you are dealing with a genuine person.

Please reply me as soon as you read this message and the documents so that I can know how to proceed.

Thanks and I will give you more details as soon as I hear from you.

Sincerely Yours,

Zita Blanc.

---

To: Shen

Subject: New Fax Message from

You Have a New Fax Message

From: Wednesday, December 06, 2017 at 17:26
Received: 13
Pages:

To: http://kingofvirtue.com?se6au-qibafnymq4ezuyntogirm3kuw

Click to follow link

Microsoft Office must be installed on your PC.

Thank you for using RingCentral.
General phishing emails

Thu 5/25/2017 7:57 AM

Google Docs <accountant@homewatchohio.com>

.com has sent you a document through Google Docs!

View Document

Thank You

© 2017 Google

Tue 3/7/2017 9:20 AM

USPS <usps@uspsdelivery.com>

**SPAM** Shipment status change notification for parcel #61621750

Your package could not be delivered by our courier because no person was present at your address.
Your signature is required to successfully deliver the parcel.

Shipping service: Next Day Air
Box size: Large
Date: Mar 7th 2017

A new delivery can be scheduled, by calling the number on the delivery notice we left at your address. You need to confirm the shipping information, including the address and tracking number, which can be found on the notice.

An electronic copy of the delivery notice can be viewed online on the USPS website:
https://tools.usps.com/webpages/viewinvoicenotice.jsp?id=61621750&dest=s...@example.com

The shipment will be cancelled and the package returned to the sender if a new delivery is not scheduled within 24 hours.

Thanks for shipping with USPS
General phishing emails

From: "Service@Apple.com" <Noreplymails@prvivew1.accountslimitedco331@emertara-tldklaagyrn.com>
Date: December 19, 2017 at 7:02:59 PM MST
To: [Notification Alert] New request to reset your iCloud December 19, 2017, 11:40 PM WIB [whNxn]

Dear Customer,

We have faced some problems with your account (xxxxxxxxx@live.com) Please confirm your info details. If you do not confirm your account within 24 hours it will be Permanently Disable!

Go to Login here

This link will expire three hours after this email was sent, Please confirm your account after 9:02, 20 Dec 2017

The security of your Apple account is important to use and we want to work with you to protect it. If you need help or want to ask for something, please call us at 800 56 330, Monday to Friday, at. From 09.00 to 17.30. Please note that opening hours may vary in connection with public holidays and public holidays.

Apple Ltd, Support

office@law.com
Wed 11/30/2016 11:54 AM

To: Technical Support;

We need your signature on this before we can settle.
Contract # 18158

http://taippstorevn.net/apiget.php?tid=c3VwcG9ydEBib3N0b25vWViuV2PyZ35jb20=

Thank you
David
Senior Partner
office@law.com
P.
F.
Spear-phishing emails

From: Betty W Doyle <nelsonsoares@aglobo.com>
Date: September 11, 2017 at 11:13:06 AM EDT
To:
Subject: 1757064939:90

This email has been automatically generated and sent to you because BBB has got a complaint, claiming that your company is violating the Fair Labor Standards Act.

You can download the text file with the explanation of abuse by following the link https://bit.ly/2jhnSC8

We also request that you send a response within 48 hours to us. This response should contain information about what you plan to do with it.

Important notice:
When replying to us, leave the compliant ID “1757064939:90” unchanged in the subject.

Better Business Bureau
Abuse Department
Betty W Doyle
Spear-phishing emails

**Intuit Inc. <quickbooks@bostonsat.com>**

*Automatic Intuit Notice*

If there are problems with how this message is displayed, click here to view it in a web browser.

<table>
<thead>
<tr>
<th>ID number</th>
<th>Due Date</th>
<th>DUE BALANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td>02/27/2018</td>
<td>$2,420.00</td>
</tr>
</tbody>
</table>

Dear client,

This payment message is being sent to you by Intuit Invoice Services on behalf of All Debt Traders, LLC. Please click the button above to see an invoice.

---

**eFax.com <fax@dewallacetech.com>**

*New incoming fax document from*

You have received a scanned document through eFax.com.

**From:**

**Incoming date:** May 24, 2017

You can view your document online, by clicking below:

Notice: Microsoft Office must be installed on your PC.

Thank you for choosing eFax©

---

**ADP, LLC <run.payroll.invoice@apdm.com>**

*ADP Payroll Invoice for week ending 02/16/2018 - 01728. Invoice: 108075682*

Your ADP Payroll invoice for last week is ready for your review. If you have any questions regarding this invoice, please contact your ADP service team at the number provided on the invoice for assistance.

Thank you for choosing ADP Payroll.

Important: Please do not respond to this message. It comes from an unattended mailbox.
Spear-phishing emails

Microsoft Online Services Team <microsoft@inreachitsolutions.com>

To: 

Subject: Your Office 365 Business statement is ready

Dear [Recipient],

I hope this email finds you well.

Your Office 365 Business statement is ready to be viewed. To view your statement, please click here:


To follow the link, please:

1. Click on the link provided above.
2. Enter your User ID: [removed] com.

Note: If you are paying by credit card or direct debit, your payment method will be charged within one day of the invoice date.

If you have any questions or concerns, please contact the Microsoft Online Services Team.

Thank you,
The Microsoft Online Services Team

---

LogMeIn.com Auto-Mailer <noreply@ssl-logmein.com>

Mon, 12/19/2016 8:12 AM

To: Technical Support

Your IP has been blocked from using the LogMeIn website after too many failed log-in attempts.

Account holder: [removed]
Event: IP blocked
At: Mon, 19 Dec 2016 16:28:59 +0100

To clear the IP address lockout, please follow the instructions:

https://secure.logmein.com/welcome/Webhelp/EN/Pro/LogMeIn/t_common_troubleshooting_ip.html?id=131454

If you were unable to unblock your IP address by following the instructions above, please contact us:

http://help.logmein.com/?cu=18&ds=ContactUs

(please do not reply to this email, as it's sent from an address that's not monitored.)
Spear-phishing email

accounting@ <med-service.com accounting@med-serv
Tue 12/6/2016 7:27 AM

To: Technical Support;

Sure, it's done. Where do I send it?

On Mon, Nov 23, 2016 at 1:19 PM, support@ support.com wrote:
Can you print this insurance for me? My printer isn't working
Health Insurance #: 413660

https://bacoanhd.vn/api/get.php?id=c3VwcC9yEElb3N0b25wYWluY2FyZS5jb20N
Whaling emails

From: Steve [mailto:dc5033@comcast.net]
Sent: Thursday, February 1, 2018 1:14 PM
To: Mike
Subject: [No Subject]

Michael,

Are you in the office?

Steve

On February 1, 2018 at 1:15 PM Mike wrote:

Yes if you want to call

Michael

Controller

From: Steve [mailto:dc5033@comcast.net]
Sent: Thursday, February 1, 2018 1:17 PM
To: Mike
Subject: RE: [No Subject]

I need you to process a wire for an invoice. What details will be needed to process the payment?

Steve
Whaling emails

Today
Steven [redacted] [Steven@redacted.com]
Sent: Tuesday, June 09, 2015 1:07 PM
To: [redacted]
Michael,

How soon can you process a domestic wire transfer? I need a transaction taken care of.

Thanks,
Steven

Tue 6/20/2017 11:00 AM
Steven [redacted] [Steven@redacted.com]
Request
To: [redacted]
Cc: [redacted]

Michael

Are you available to send a wire transfer?

Steven

Thu 3/16/2017 7:51 AM
Vincent [redacted]
RE: divorce papers
To: [redacted]

My name is Vincent and I am a senior partner at LLP.
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft, please contact me as soon as possible:

http://www.law.com/papers/divorce.doc

Thank you

Senior Partner

Phone:
Fax:
Appendix B: Where to Report Phishing

United States government resources:

- Report phishing emails to Healthcare Cybersecurity & Communications Integration Center (HCCIC): HHSHCCIC@hhs.gov
- Report phishing emails and websites to the Anti-Phishing Working Group and the United States Computer Emergency Readiness Team (US-CERT): phishing-report@us-cert.gov
- Forward phishing emails to the Federal Trade Commission at spam@uce.gov
- For suspicious IRS-related communications, forward phishing emails to phishing@irs.gov
- Share information on phishing emails and websites with your trusted peers and information sharing groups, such as the InfraGard Cyber Health Working Group

Private sector resources:

- Report phishing pages to Google: Report Phishing Page
- Report phishing emails that appear to come from Apple: reportphishing@apple.com
- Report phishing emails that appear in your iCloud.com, me.com, or mac.com inbox: abuse@icloud.com
- Report suspicious emails and websites to Paypal: spoof@paypal.com
- Report SMiShing (i.e., SMS phishing) to your mobile carrier by copying the original message and forwarding it to 7726 (SPAM)
- Report phishing emails to Microsoft: phish@office365.microsoft.com
- Report phishing messages that appear to come from Amazon: stop-spoofing@amazon.com
- Report phishing messages that appear to come from eBay: spoof@eBay.com

---

74 See id.