CYBERSECURITY THREATS: PROTECTING YOUR ORGANIZATION

How to Identify Fraudulent Email Attacks

Authors: Nick Holcomb and Eric Whisenhunt

Payroll Network℠
Simplifying Human Capital Management

Email is a vital communications tool for business, but also presents a security risk as its open nature and widespread use makes it a rich target for malicious actors. Previously, email attacks took the form of worms and viruses, which would attempt to deploy harmful software to a users' PCs and then spread rapidly across the local network. Today, the objective of most email attacks is to commit theft – actual fraud involving money transfers.

TYPES OF EMAIL ATTACKS

SPOOFING

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites.[1] It is a low-tech attack, is easy to perpetrate, and can be hard to prevent without the right tools and understanding.

These will often take the form of emails that appear to originate from the organization's CEO or COO. The sender's name is valid, but a closer look at the email shows that the sender email address is invalid. The target is usually the CFO or someone employed in the accounting department who may have authority to pay invoices or initiate money transfers. Names and email addresses of possible targets are obtained from various sources, such as a company's website or social media accounts, such as LinkedIn.

Diagnose & Prepare

Examples of a spoof attack include:

- Emails to HR/payroll requesting Direct Deposit changes.
- Emails to HR/payroll requesting copies of W-2 forms.
- Emails to the CFO from the CEO requesting an urgent money transfer.
- Emails to someone in the accounting department that contains a fake invoice as an attachment.

Ways to prevent falling victim to spoofed email attacks:

- Educate individuals responsible for monetary transactions (payroll, HR, accounting) about current risks.
- Institute policies preventing changes to the movement of monies without secondary authentication, for example:
  - » Require employees to use the payroll/HCM system to request Direct Deposit changes. This is more secure than email as it requires the user to authenticate to the HCM system.
  - » Require voice authentication before following through with a request. Have your associates call the initiator to verify the authenticity of the request.

Compromised (Hacked) Email Accounts

A compromised email account can result in fraudulent requests similar to Spoofed emails, but they are much harder to identify as the email is coming from a legitimate email account. The account is being operated by a malicious actor (hacker).

Recognize & Verify

Examples of hacked email attacks include:

- Emails to HR/payroll requesting special payroll processes, with new fraudulent payees.
- Emails to HR/payroll requesting Direct Deposit changes to existing highly compensated employees.
- Emails to the CFO from the CEO requesting an urgent money transfer.
- Emails to someone in the accounting department that contains a fake invoice as an attachment

To prevent falling victim to email hacking attacks:

- Use Multi-Factor Authentication (MFA) to access the email system which will help prevent your employees from having their email account compromised by a malicious actor.
- Educate individuals responsible for monetary transactions (payroll, HR, accounting) about current risks.
- Institute policies preventing changes to the movement of monies without secondary authentication, for example:
  - » Require employees to use the payroll/HCM system to request Direct Deposit changes. This is more secure than email as it requires the user to authenticate to the HCM system.
  - » Require voice authentication before making changes. Have your associates call the requestor to verify the authenticity of the request.

PHISHING

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.[2] According to the FBI, phishing-based emails have generated $12B of wire fraud since 2013.[3]

Be Aware & Report

These will often take the form of an email request to click on a link that will direct the user to an authentic looking, but fake, login page. If the user is fooled, and enters their username and password, the Bad Actor now has a copy of the credentials. Multi-factor authentication foils this type of attack by sending a six-digit code as a text to the user's mobile phone. The code must be entered, in addition to the username and password, in order to gain access to the email account. Without possession of the phone, the Bad Actor cannot gain access despite having obtained the user's email credentials.

To prevent falling victim to email hacking attacks, end-users should not click on links or attachments embedded in unsolicited emails. In other words, unless you are expecting something from a sender, don't click. Instead, forward the suspicious email to your IT department for further review.

Conclusion

Email threats will continue to evolve and victimize end-users in unexpected ways. In order to protect your organization from fraud and data loss, establish policies to confirm the authenticity of any request to transfer funds, pay an invoice, or provide copies of private information, such as a W-2 form.

Consider implementing a cybersecurity awareness training program for your employees. Ensure that your organization uses a modern, secure payroll/HCM system to process payroll and HR changes. Protect your email system by implementing additional layers of defense, such as multi-factor authentication, DNS-based email link filtering, and real-time endpoint security agents that detect and prevent the downloading of malicious software to a PC.

Nick Holcomb is the Chief Technology Officer for Payroll Network, a premier HCM provider that brings together key workforce functions in one robust, easy-to-use platform. Nick has more than 20 years background in cybersecurity and 15 years of payroll/HR industry experience.

Eric Whisenhunt is a Principal with Computer Showcase, an IT solutions provider offering strategic consulting, managed services, and cloud solutions. Eric has been helping organizations embrace new technologies to improve capability, efficiency, and data security for more than 25 years.

---

1 https://www.forcepoint.com/cyber-edu/spoofing
2 https://www.phishing.org/what-is-phishing
3 https://www.inky.com