StratumPoint
Situational Awareness for More Effective Decision Making™

Understand, Identify,
Meet, and Defeat

Social Engineering: Identification, Impact, Defense and Response

Malcious Exploitation of Inherent Human Vulnerabilities

Steve Hinton
Principal, Intelligence Operations
StratumPoint, Inc.

STRATUMPOINT
Situational Awareness for More Effective Decision Making™

Social Engineering

#1 Threat in Today's Cyber Landscape

84% Estimated number of cyber attacks that are enabled through some form of social engineering

$6 Trillion

Estimated damage costs of cyber crime annually by 2021

70%

Percentage of cyber attacks that employ social engineering to enable more advanced hacking

$38.5 Billion

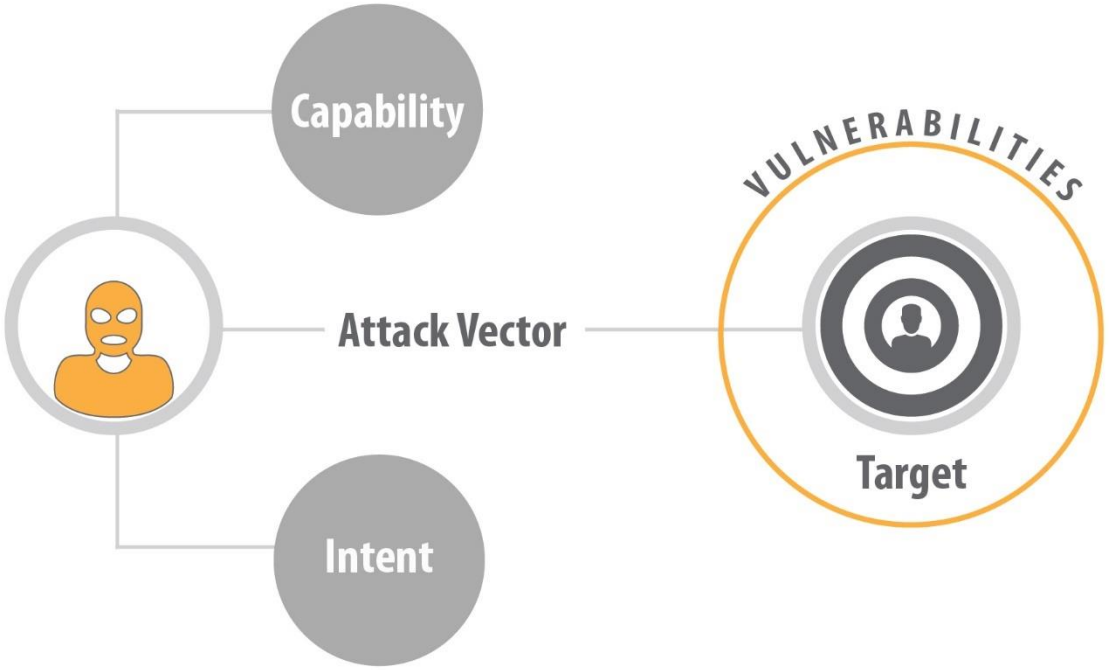
The cost of the most expensive computer virus currently on record and was transmitted via a social engineering attack

SOCIAL ENGINEERING: Overview

Human Nature.
Inherent Vulnerability.

Social Engineering is an inherent part of human interaction. Not all social engineering is nefarious, however from a protection perspective, it can include:

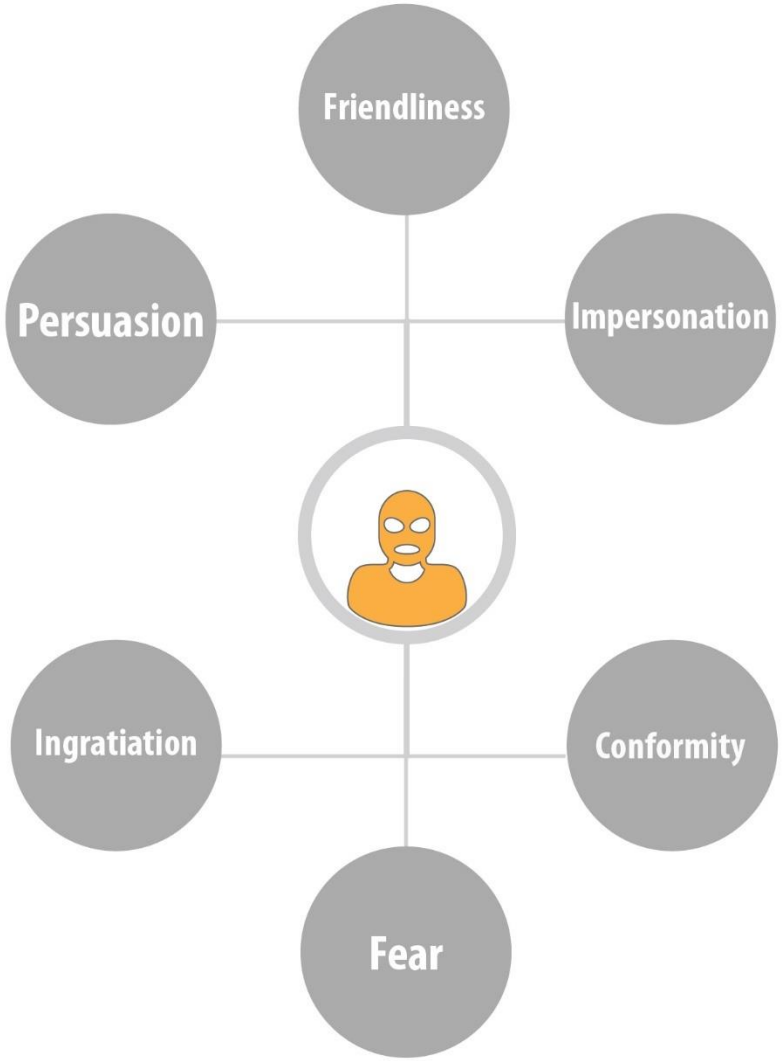
- Using influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation
- Human interaction (personal, telephonic, digital, etc) whereby a person reveals information they otherwise would not.



Social Engineering and Cyber Attacks

There are multiple components that make up a cyber attack. Understanding these, and how they interact within your organization is the first step for social engineering attack vector recognition that threaten operations and the critical data it contains.

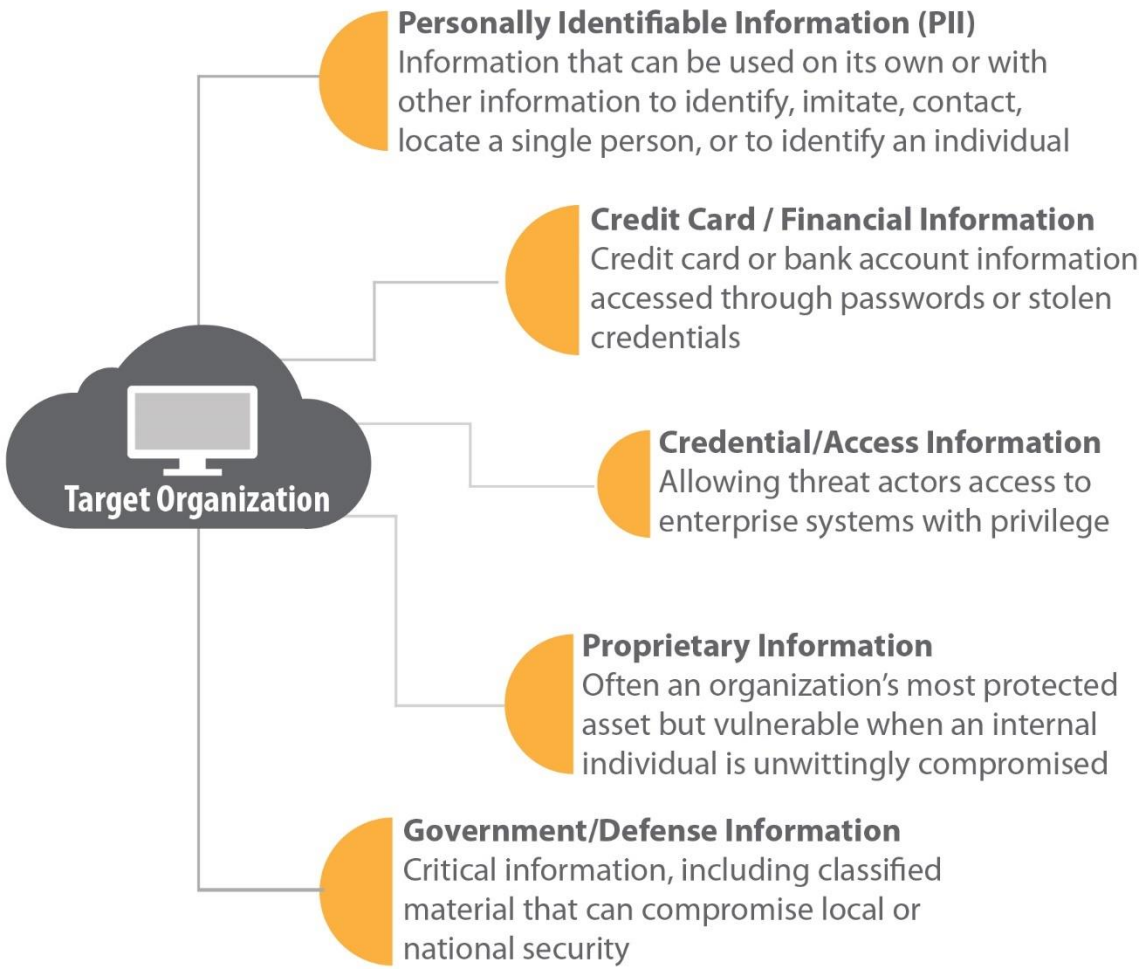
Social engineering is the most prevalent access vector to gain access and enable an attack.



Social Engineering and Time-Tested Techniques

Social engineers use a variety of tools to manipulate their targets. Although the mediums of social engineering have expanded, the techniques employed are proven effective.

In general, people have a tendency to trust and develop a connection with others. Through social engineering, malicious actors are exploiting this vulnerability for a variety of end goals across the spectrum of targets.



Targeting: What and Why

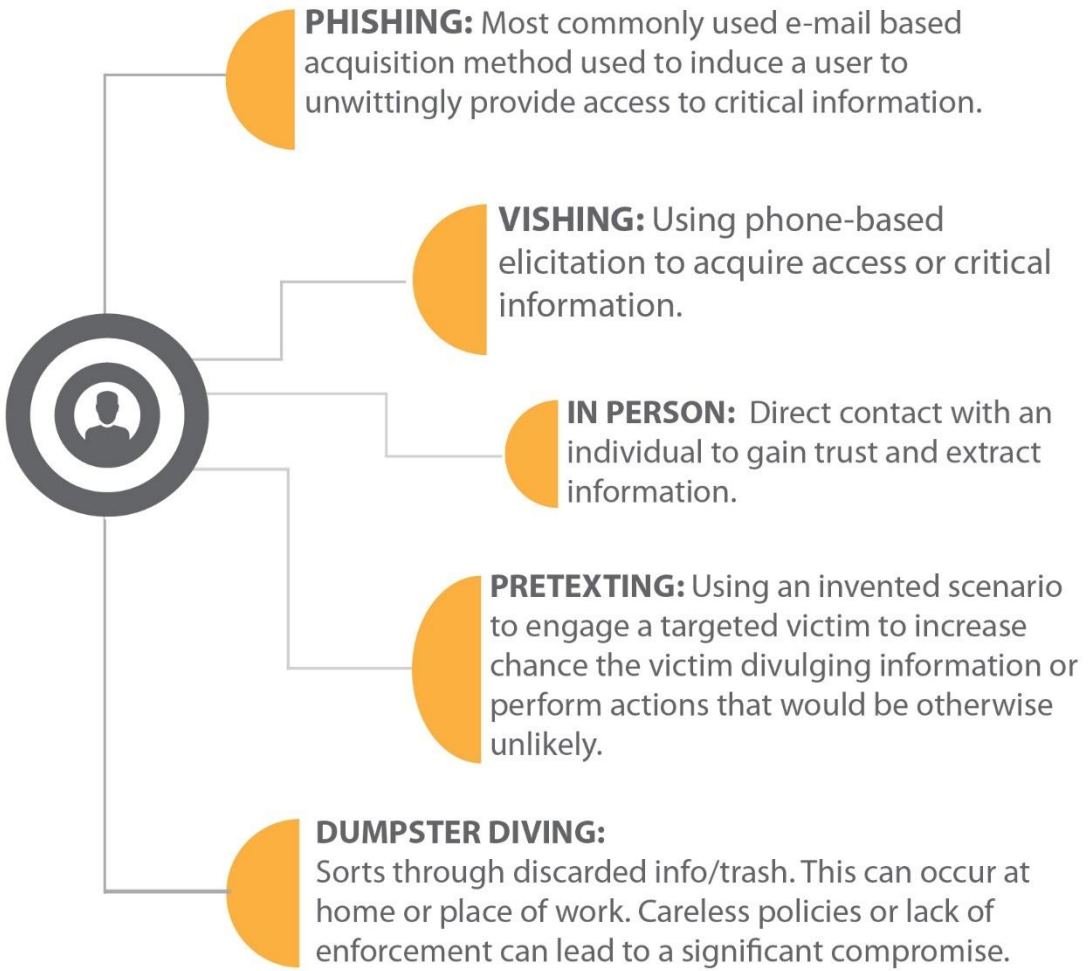
Different threat actors focus on different targets based upon desired end state. Different industries vary on the full scope of their exposure, however all industries have some threat actors and attack vectors in common.

Motivations vary from target and threat actor and range from financial profit, to revenge, to foreign national interests.

Targeting: Who

Malicious actors target different people in different roles for specific purposes. The spectrum of targets experience a variety attack vectors based on assessed access to desired target data. Targets include:

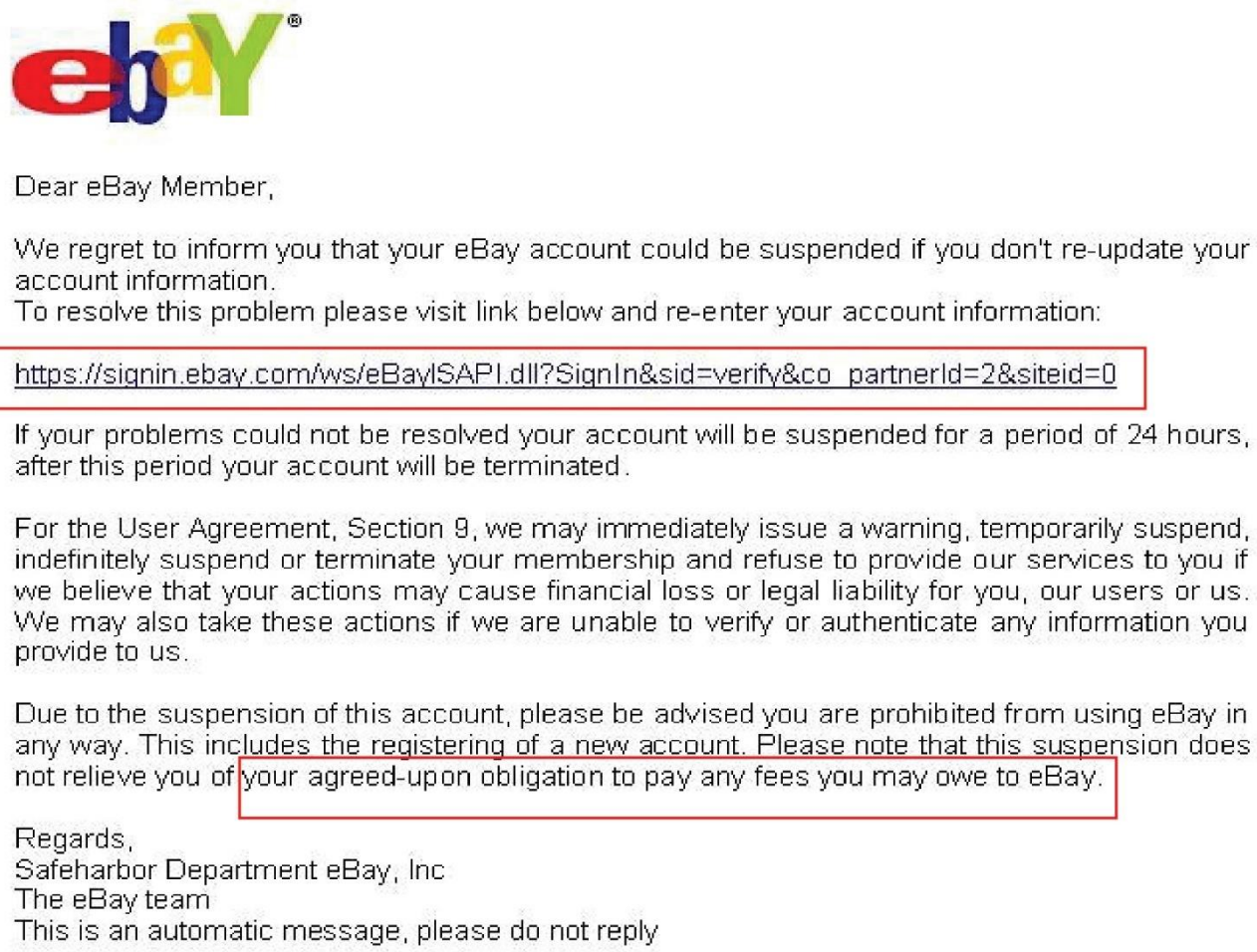
- Students
- Faculty
- Receptionist
- Finance
- New Hires
- Executives
- Human Resources



Targeting: How

Bad actors focusing on social engineering have many tools at their disposal. Some leverage bleeding-edge technology while others are more archaic but tried-and-true.

Threat acors will action their tactics based on multiple factors including assessed vulnerabilities, geography, organic skillset, and requisite access based on end goals.



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

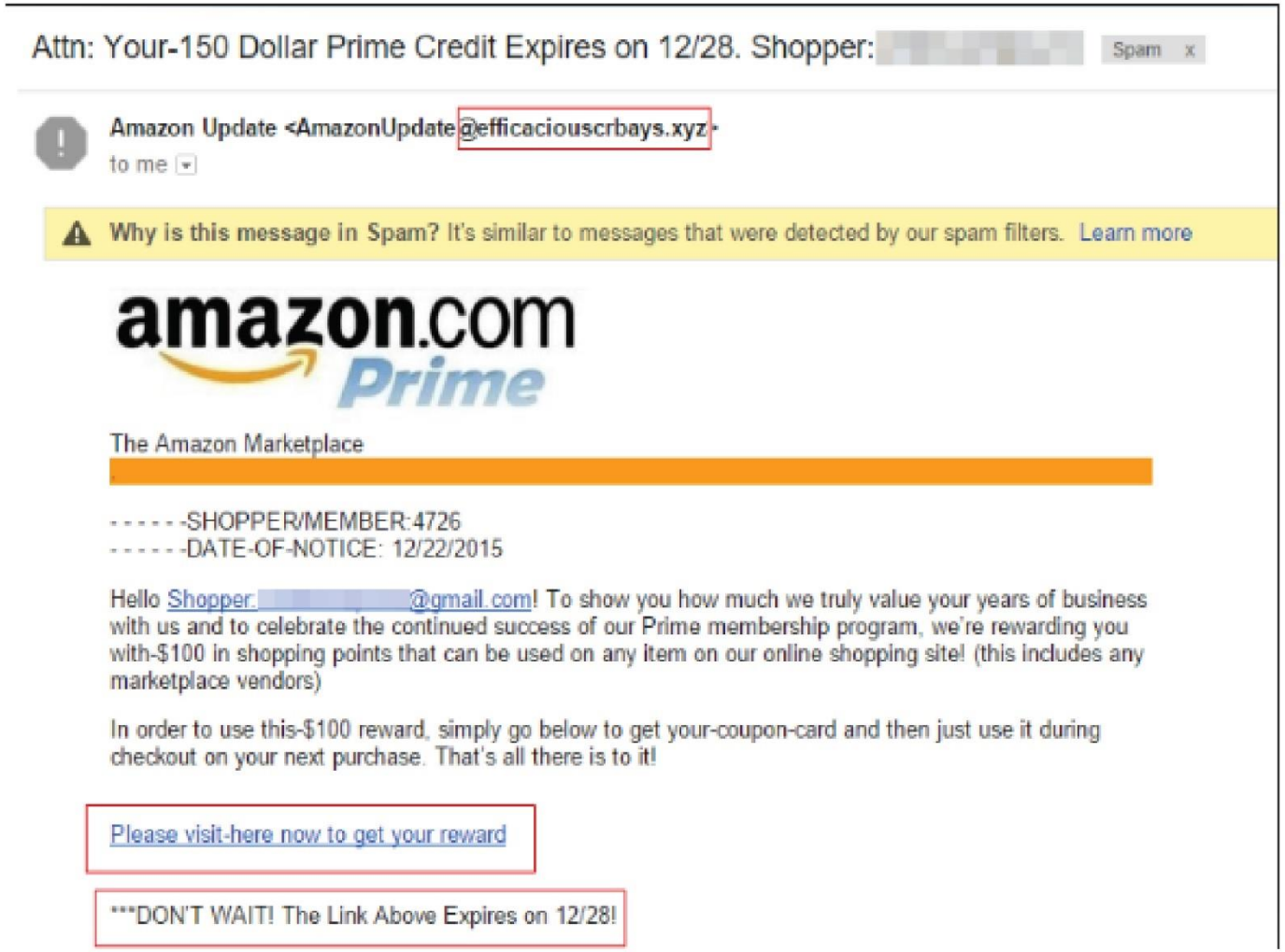
Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Attack Recognition: Spear Phishing

Phishing and Spear Phishing are e-mail based attacks that are pervasive and effective. The spear phisher relies on familiarity and weaponizes it against their victims.

NOTE: Fear for potential disconnection of the user's account as well as potential implications of financial obligation may pressure the user to click the link and likely install malware.

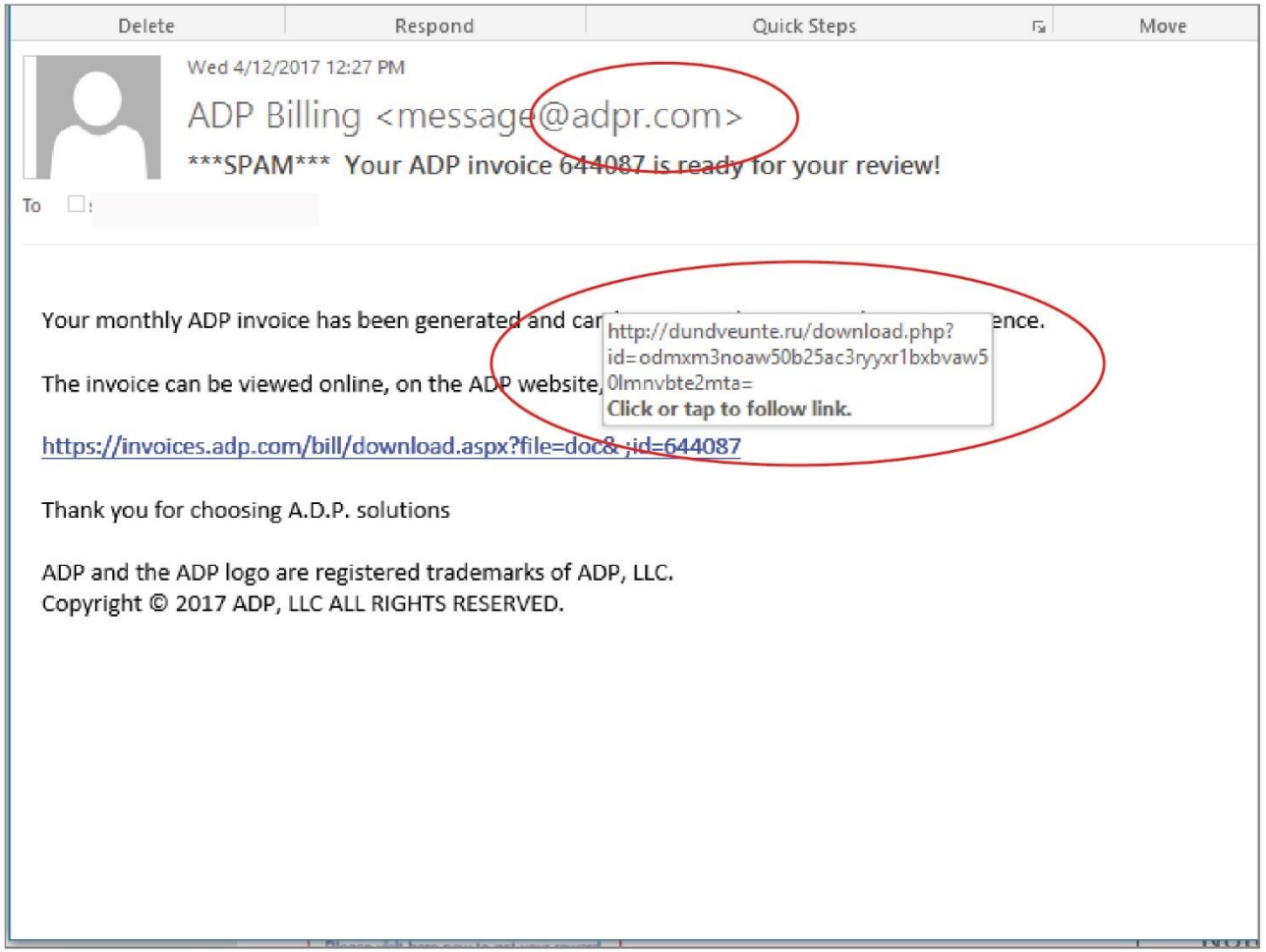


Attack Recognition: Spear Phishing

Spear phishing attacks are becoming increasingly sophisticated and can replicate common communications from trusted sources to appear authentic.

Looking at the actual e-mail address (or hovering over the link to reveal the true address and help stop the attack before it can do damage.

NOTE: The use of urgency and reward



Attack Recognition: Spear Phishing

This recent example plays on familiarity of a trusted business with whom the target may or may conduct current business. It appears legitimate in content with no obvious spelling/grammatical errors

NOTE: Hovering over the link reveals it does not link to ADP, but rather a Russian detsination. Clicking on this link would likely install malware.

Attack Recognition: Spear Phishing

The CEO/CFO wire transfer scam netted social engineering criminals billions of dollars in 2016. Attackers conduct extensive research for targeting and rely upon employees to follow instructions from senior leadership. While it takes more effort from the attacker, it is highly effective when researched and executed properly.

Do you have a moment? I am tied up in a meeting and there is something i need you to take care of.

We have a pending invoice from our Vendor. I have asked them to email me a copy of the invoice and i will appreciate it if you can handle it before the close of banking transactions for today.

I cant take calls now so an email will be fine.

Sent from my iPhone

Social Engineering: Defense

There are several steps that personnel and organizations can take to further harden their attack surface against social engineering attacks; but steps must be taken by all and reinforced regularly. These steps include:

- **TRUST BUT VERIFY.** When a potential social engineering attempt appears to be in play, externally verify through proper vetting practices and strong communication.
- **PASSWORD COMPLEXITY.** Effective password complexity is essential. Additionally, two-factor authentication is highly encouraged.
- **AWARENESS and TRAINING.** Regular training should be reinforced and in line with best security practices as well as organizational policy guidelines.
- **COMMUNICATION and VIGILANCE.** Always be communicating with others in the organization. Reporting a potential attack is good, but ensure the lessons-learned are disseminated so that others in the organization are sensitized, which will harden your attack surface.

Social Engineering: Response

It is not a matter of IF, but WHEN users will be targeted for a social engineering attack. When an attack appears to have occured (whether the user is positive or not), it is recommended to:

- **REPORT.** Follow organizational procedures for reporting an incident, however, the IT department is a smart starting point for e-mails or a direct supervisor for telephonic or in-person attempts.
- **NOTIFY OTHERS.** Ensure others are aware of the attack and help them to understand and recognize the signs so they do not fall victim.
- **BE FORTHRIGHT.** Users must be encouraged to report an attack, even if they may have fallen victim and clicked a malicious link. This aids in remediation. Organizations must reinforce the need for this level of openess and employ a policy that encourages such candor without fear.
- **DEVELOP and ENFORCE EFFECTIVE POLICIES.** Enforcing effective policies is paramount, however they must be somewhat dynamic to adapt to emergent threats and new attack vectors.

Social Engineering. Final Thoughts

You are charged with the protection of critical data that is under persistent attack from cyber threat actors conducting social engineering to exploit it for nefarious purposes. Take responsibility. Be vigilant.

- In the asymmetric cyber landscape, EVERYONE is a gatekeeper of critical information
- Security is part of ALL departments and roles within an organization, not just the IT department
- Vigilance will result in a more secure organization

Contact Us

Please contact StratumPoint with any questions or any additional ways we can be of assistance.

Steve Hinton
Principal, Intelligence Operations
Shinton@StratumPoint.com
(877) 250-8520 Ext 701

Rebekah Brown
Principal, Cyber Operations
RBrown@StratumPoint.com
(877) 250-8520 Ext 706

StratumPoint, Inc.
877-250-8520
www.StratumPoint.com
Info@StratumPoint.com