Spear Phishing

SPEAR PHISHING: UNDERSTAND, ANALYZE AND PREVENT

What is Phishing?

Phishing is a social engineering technique that aims to deceive people into unknowingly providing their personal financial information or other type of credentials to cybercriminals. A phishing attack is most often initiated with a type of unsolicited email that prompts the user to click on a link with the purpose of misleading users into what appears to be a legitimate website. A phishing email tricks the recipient into visiting a spoofed site—one that mimics a legitimate site where the person would normally feel comfortable entering a username, password, credit details or other type of private information.

Spear Phishing vs Phishing

Both attack types are focused on acquiring confidential information. Phishing is a broader term for any attempt to trick victims into sharing private data and credentials for malicious reasons. Attacks are not personalized to their victims, and are usually sent as bulk mail to full email databases.

Spear phishing attacks try first to obtain as much personal information about their victims as possible – this gives the effort much more credibility and increases the likelihood of catching the victim. These more sophisticated techniques target a specific individual or group with some sort of "individualized" details in the message. Because of the trust factor of personal emails, it is more difficult for recipients to identify spear phishing attacks than basic phishing.

Spear Phishing on the rise

Spear phishing is on the rise. Why? Because it works. Traditional filtering techniques tend to analyze messages in conventional ways to identify unwanted or nuisance emails, but struggle to correctly flag spear phishing attempts.

For fraudsters, spear phishing is the perfect vehicle to target executives by tricking them into either providing their credentials or using them as a stepping stone to reach other employees, leveraging the credibility inherent to executive communications throughout the messaging process.

Spear phishing attacks aren't always restricted to collecting private information though. Often, they will also be used to plant ransomware into the network that encrypts company data, then extorts fees from the victim to remediate the situation. Other attacks focus on point-of-sale reconnaissance trojans that target businesses primarily in the retail and hospitality industries.

> *"About 80% to 90% of the data breaches that my team sees go the phishing route."*
>
> Andrew Conway
> Microsoft's General Manager
> for Microsoft 365 Security

Spear Phishing Trends

Attacks continue to grow more customized, whether through an attempt to deliver malware or to perpetrate a phishing attack. However, spear phishing tactics continue to net attackers huge sums as Business Email Compromise (BEC) attempts and other social engineering fraud are becoming much more widely adopted by attackers.

Broader scale attacks

Spear phishing has become so much more common and is being seen with a much greater frequency than ever and is being delivered on a much broader scale.

Perhaps even more concerning is the fact that a great deal of these attacks are being launched from trusted sources that are usually compromised accounts. These attacks are designed to disarm email security measures that focus on sender validation.

Specifically, looking for spoofed domain names, bad IP reputation and things like DKIM and SPF will all generally fail to raise any red

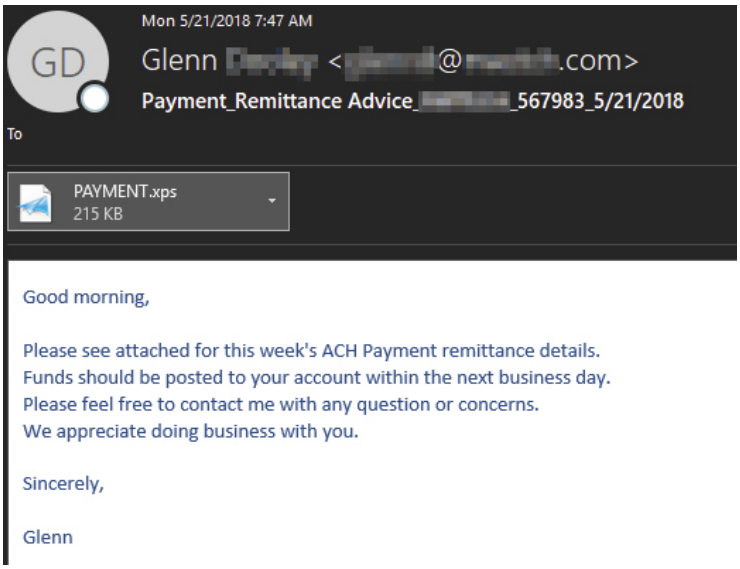
flags. These attacks also have great success in subverting well trained end users who might otherwise be cautious enough to avoid emails from unknown senders.

How does it work?

The process starts when cybercriminals identify victims who put personal information on the internet or have personal data published online. Criminals may then complement some relevant data by browsing individual profiles while scanning social networking sites. Once they have an identity, collecting the email address is fairly easy since there are many online services that not only provide email addresses for each individual but also will test and confirm that the email is in active use.

Spear Phishing Example

Our Advanced Email Security filtering captures a wide range of these types of phishing messages.



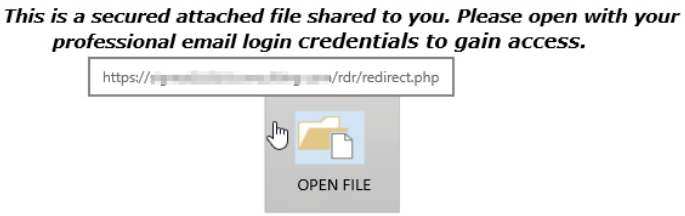
So far, most appear to be attributed to threat actors currently conducting BEC attacks. Attacks appear to originate from legitimate (compromised) senders with similar techniques, tactics and procedures.

Viewing the XPS File

Users should not open or view unsolicited attachments, even from a known sender, without intense scrutiny and/or verification. Scammers intentionally exploit the trust that known contacts share and hopefully, you or your users will never see one of these types of attacks. However, this is what these attached files look like when opened in an isolated test environment.

Linked Phishing Portals

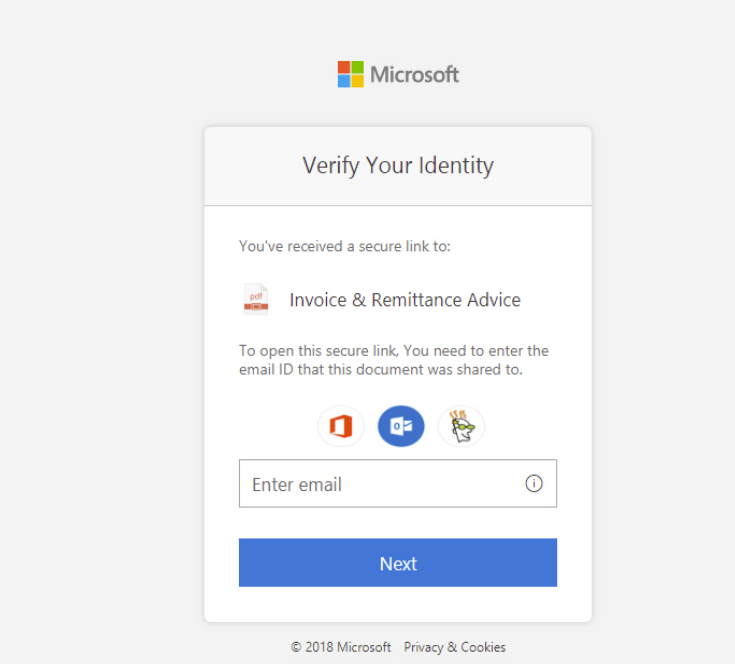
If the user happens to click on the link in the



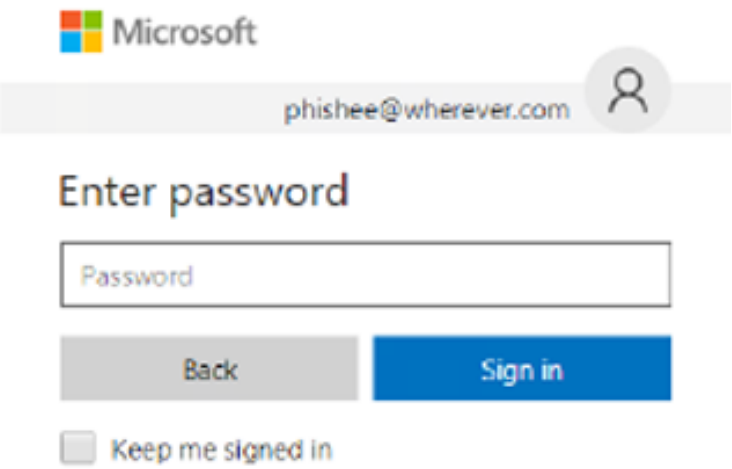
attached xps file (pictured), below is an example web phishing portal they might encounter. For this particular one, the first screen requests an email address. If they proceed, the next image shows the resulting page requesting further email credentials.

Spear Phishing

Request for Further Credentials



After entering email address

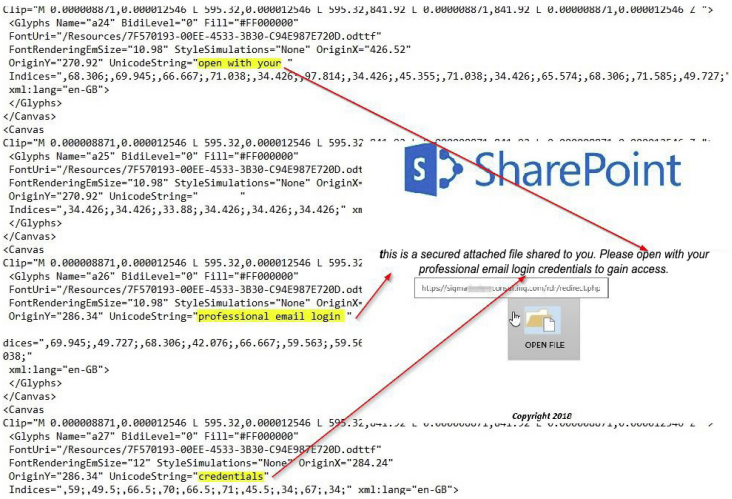


Filter Evasion Techniques

Malicious actors are constantly attempting to find the most effective filter evasion techniques. They break up the suspicious phishing text via canvas clip mappings inside deeply embedded fpage files. An image portion displays how cybercriminals use multiple canvas clip mappings to stitch together the words, "open with your professional email login credentials."

Minimal AV Signatures for XPS Files

Most anti-virus engines do not have many phishing rules established for the xps extensions as they would for more commonly used extensions.



Protection and Best Practices

Better Email Security

Organizations need an email security solution that automatically detects and blocks advanced targeted spear phishing campaigns. AppRiver's Advanced Email Security delivers a unique email security solution that is more effective than standard solutions, and which proactively protects organizations from email-based cybercrime by merging advanced big data security, dynamic rules and security analyst expertise in order to anticipate the next wave of spear phishing techniques. It is imperative for full content inspection to be implemented and that every aspect of the email be evaluated using a multitude of techniques.

Multi-layered Security

Securing a network with a multi-layered approach is a best practice.

Your organization should protect all security fronts by combining email and web security solutions with an endpoint AV protection layer. Web security platforms, such as AppRiver's Web Protection, will complement email security and AV endpoints by not only blocking malware at the source, but also by scanning networks in search of resident malware that went untraced in the past that could potentially be calling home under the right circumstances.

By deploying the right combination of email protection, endpoint AV and web security, your business can close the security gaps present in each network and gain inbound and outbound traffic monitoring.

Audit your Security

Every business, including yours, has valuable IT assets such as computers, networks, and data. Providing adequate and effective protection of those assets requires that companies of all sizes conduct IT security audits to get a clear picture of the status of their network, become aware of the security holes they face and learn how to best deal with those threats.

Contact us for a tailored security audit and threat analysis report that will provide you with critical information on the health of your email or network and also provide our recommendations on the best ways you can plug any identified security holes.

Limit User Rights

Some malware can be installed unknowingly by employees at the same time as other programs are downloaded. This may include software from third-party websites or files shared through peer-to-peer networks.

Therefore, it is important to limit user rights as they pertain to the installation of software.

Security Tips for employees

With the popularity of spear phishing on the rise, it is always good advice to provide some tips and best practices to keep your employees aware of security threats.

Password complexity

Never stick to one single password for all your services! Instead, use different combinations for each service, use passwords with at least 8 characters, although 12 or more is recommended. Passwords should also be a random combination of uppercase and lowercase letters, numbers and symbols. A password manager can also help by managing multiple accounts and suggest strong password options.

Stay alert for suspicious links
Only click web links within emails you know to be authentic. If an organization, such as your bank, asks you to perform any activity that involves clicking links and entering credentials, either launch your browser and go directly to the bank's site or just call them up to double check on it. Hovering your mouse over a link will always give some insight on whether the link could be spoofed and be fraudulent. However, some attackers try to obfuscate link destinations by using anchor text trying to look as a legitimate URL or URL shorteners to disguise the ultimate link destination. It's best to always assume the worst when it comes to following links.

Employee Training Programs
Implement a course on security awareness and social engineering techniques that will help your users make better judgments about the content they download from the internet, receive through communications and access through the Web.

Security awareness training will also help users to be more careful about what they view, what they open and the links on which they click.

While training by itself will not completely solve an organization's security-related problems, it adds to the overall defense strategy by increasing the layers of security for the weakest element – humans. It will bolster the ability for users – the LAST (not first) line of defense in any security infrastructure to be more aware of malicious attacks against themselves and the organization.

Search yourself online
Be extra cautious when sharing data on social networks and limit what types of personal information you post on the internet: Review your online profiles and ask yourself how much personal information is available for cyber criminals to view? If there is anything that you do not want a potential scammer to see, do not post it – you should also consider reviewing your privacy settings on sites such as Facebook and Twitter to limit what information is left open for others to see.

appriver.com
sales@appriver.com
(866) 223-4645