Email Security

# understanding email security

## Phishing

What is 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, credit card details, and passwords.
* Phishing emails typically look normal and can sometimes be hard to spot. Always verify the sender, and if it is an unexpected email, or you are unsure, then contact IT.
* These attacks may also impersonate someone you know, a boss, co-worker, friend or family member.
* The top 10 impersonated organizations in phishing emails from 2018 are:
  + Google (15.6%)
  + Microsoft (10%)
  + Dropbox (9.8%)
  + PayPal (8.9%)
  + Apple (8.2%)
  + Adobe (7.5%)
  + Facebook (7.3%)
  + Wells Fargo (6.5%)
  + Bank of America (4.4%)
  + Yahoo (4%)
* More information on spotting and identifying these attacks will be in a later section.

## Email Attachments

Hackers and phishers often send unsafe or malicious email attachments hoping that a user will download or open them on their computer. These attachments typically contain malware that will execute on your computer which can allow the hacker to steal your personal information, take your files for ransom, or spy on your activity.

* Always pay attention to the identity of the sender and verify the type of attachment that is being sent. Common malicious attachments usually have the following file types: .exe, .cmd, .bat, .msi, .psc1, .vb, .vbs, .js
* If you receive a suspicious attachment or unexpected file, please contact IT.
* Some malware sent as email attachments can even infect your entire company. It is always important to pay very close attention to what you are downloading

## The Importance of Multifactor Authentication (MFA) or Two Factor Authentication (2FA)

What is Multi-Factor Authentication?

* Multi-Factor Authentication is an additional layer of security for account authentication. When using Multi-Factor Authentication, a user is required to enter an additional piece of information when logging into their account. The additional information could be a one-time code that is sent over a text message, a string of numbers on an authenticator application or device, or a phone call.
* With Multi-Factor Authentication, it is much harder to gain access to an account that may have had its credentials compromised. This is because of the independent security token that is required to sign in or make changes to the account.

Social Engineering

## Phishing

A more in-depth look at Phishing, one of the most common types of social engineering.

There are many types of Phishing

## Classic Phishing

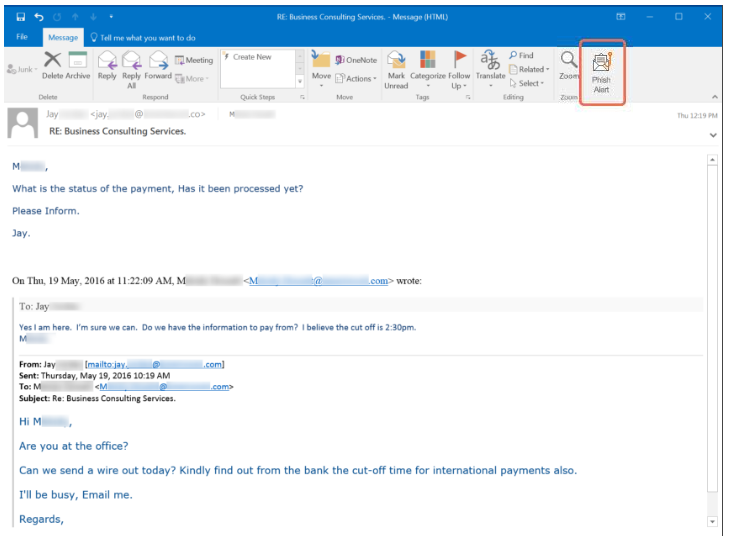
* Mass emails, sent to as many people as possible, generic looking, usually impersonating a company and asking for account information or reporting a fake problem with your account.
* The typical “Prince from India” scam.

## Spear Phishing

* A more personal approach to phishing. The hacker usually researches the company or user and includes specific information about the company or user in the attack.
* May include information about certain vendors you are using, or employees of the company.

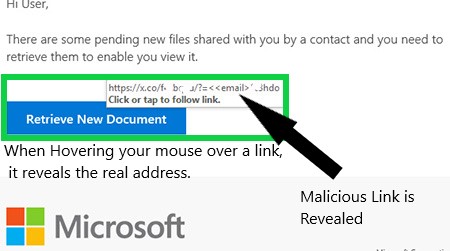
## Whaling

* A phishing attack that is targeted at high-profile employees. (CEO, CFO, President, Vice President)
* Usually contains very specific information and can be extremely convincing. It is important for high-profile employees to confirm requests and transfer of information with their contacts outside of email.



## Link Manipulation

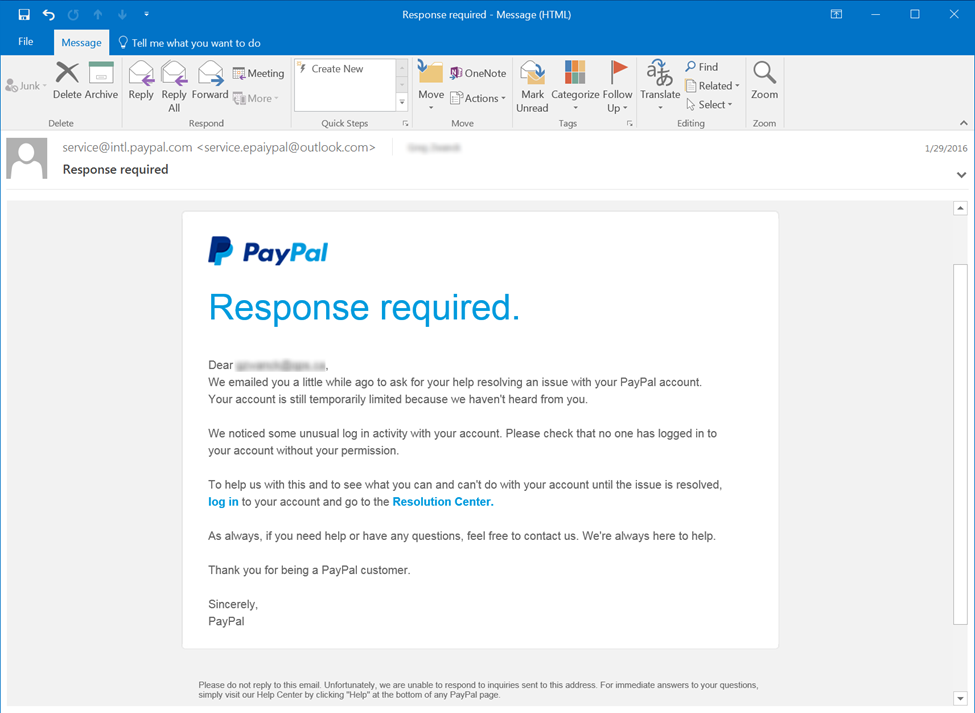
* The hacker sends a malicious link which redirects the user to a site. The site may request account information or download a malicious file.
* The displayed link does not always redirect you to the expected destination.
* Hover your mouse over links to verify the true destination.



.

## Malware Phishing

* Typically contains a file or attachment that needs to be downloaded onto the computer, so the hacker can take control and steal information.



## Vishing (Phone Phishing)

Vishing or “Phone Phishing,” is an alternate method of social engineering used to obtain information, personal/financial records, money, or a request/action from a user via phone. The “Visher” usually pretends to be IT, a company employee, an outside vendor, or even a customer.

* Always verify the identity of callers if you are not 100% sure who they are.
* Never give sensitive information to callers unless their identity has been verified.
* Visher’s usually portray a sense of urgency because they are trying to invoke the emotions of the target, which can coax the target into making a quick decision.

Viruses and Malware

# An Overview of Malware

## General Malware Prevention Tips:

* Make sure you are using a reputable anti-virus program like Webroot.
* Be very careful when installing programs, and make sure they are from a reputable developer.
* Pay close attention to what links you click in emails and on the web.
* Keep your operating system and programs up to date. (Flash Player, Java, etc.)
* Stay away from illegal websites. (software pirating, “free” TV and movie streaming)
* Do not run or install unknown programs just because you are prompted to.
* Don’t use out of date operating systems like Windows XP or Windows 7. (end of life in 2020)

## Worms

* Malware that can reproduce itself, and typically needs you to execute a program.
* Reproduces through file systems or network.
* Can infect an entire network in seconds.

Preventing Worms

* Be very careful when downloading and installing software.
* At home: Make sure you are using firewalls and they are up to date. (Most at home routers have a built-in physical firewall)

## Ransomware

* Locks your computer, encrypts your files and then holds them for ransom.
* Can spread to the entire network and encrypt other computers.
* Sometimes it is impossible to remove the encryption.

Preventing Ransomware

* Keep your operating system, anti-virus, and applications up to date.
* ALWAYS keep backups of your data. (Ideally an offline backup)

## Trojan’s

* A trojan is a type of rogue software that pretends to be something else (fake anti-virus software), so it can take over your computer.
* It is purposely built to avoid Anti-Virus software and avoid detection.

Preventing Trojan’s

* Verify that you are downloading reputable software from and verified vendor or developer.
* Only download software and applications from the vendor or developer’s official website.

## Rootkits

* Modifies the core files of the system.
* Can be invisible on the computer.

Preventing Rootkits

* Use Anti-Virus Software and don’t download unknown applications.

## Keyloggers

* Records your keystrokes and sends it back to the hacker.
* Saves all keyboard inputs with the hopes of stealing account and credit card information.

Preventing Keylogger’s

* Always use Anti-Virus software with real-time protection.

## Adware and Spyware

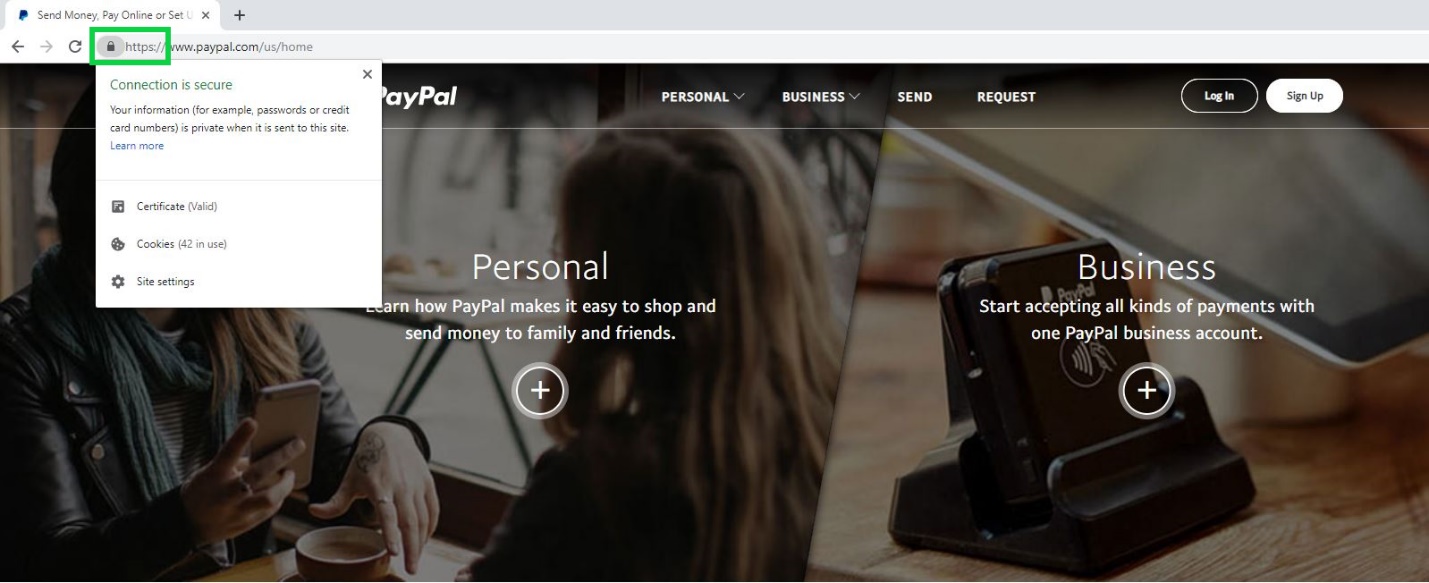
* Frequent pop-ups and advertisements.
* It is sometimes installed as a browser extension or with a program.
* Captures web surfing habits and can record keystrokes.

Preventing Adware and Spyware

* Be careful when downloading browser plug-ins and extension.
* Maintain your anti-virus software.
* Stay away from illegal websites.

Safe Web Browsing

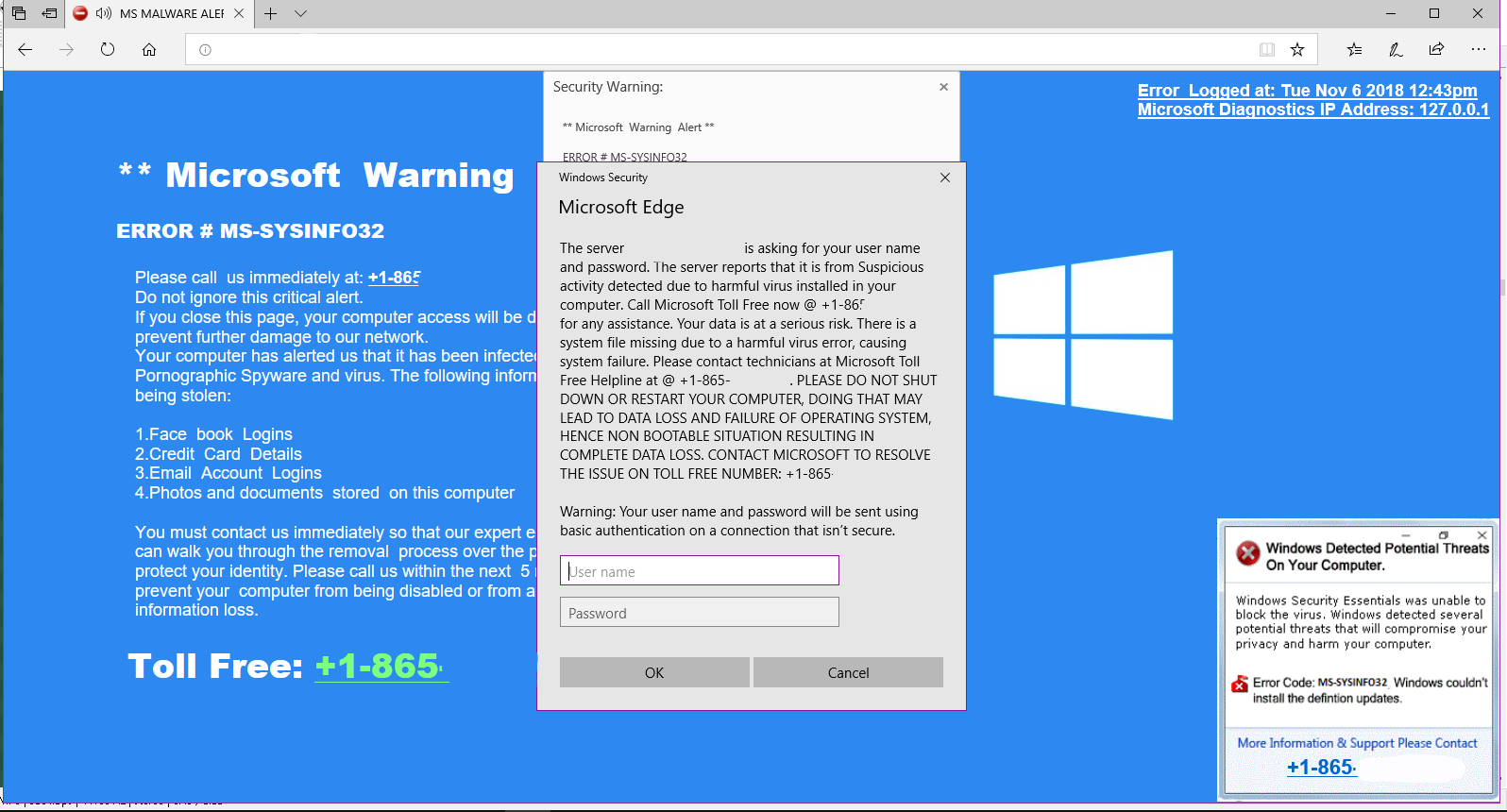
## Risky Websites

* Adult content, software piracy, and gambling websites are commonly filled with adware and other malicious content.

Never enter account information or important information on a website that isn’t (HTTP) HTTPS. Look for the lock sign next to the URL; this means that the web site is using HTTPS and is more secure.

* HTTPS means that all information you type on the website is encrypted when sent back to the web server.

## Browser based Hoaxes

* One of the most common occurrences of a browser-based hoax is the “Fake Tech Support Scam”.
* A user receives an alert on their browser that their computer is infected and they a usually prompted to contact 3rd party (fake) support.
* Can be difficult to close out of, use Control+Alt+Delete and end the task of the internet browser.
* Cross Reference hoaxes on websites like https://www.hoax-slayer.net

Password Security

# Maintaining Password Security and Best Practice

### A password is a string of characters used to prove identity or access, which should be kept secret from those not allowed access.

## Don’t Re-use Passwords

* Using the same password for multiple accounts can lead to other accounts being hacked if your account information has been involved in a data breach.
* On December 5th, 2017, a list of unique accounts and passwords from various data breaches was found and is available to the public. This list contained a total of 1,400,553,869 unique accounts.
* The information in these data breaches can potentially be used to recover your accounts if you use the passwords for other accounts.

## Strong Passwords

* The use of unique and random passwords significantly reduces the possibility of an account being breached in various types of attacks.
* A password should contain at least 12 characters containing upper case, lower case, numbers, and symbols.
* Change your passwords periodically.

## Protecting your Passwords

* The use of a password manager like LastPass can help you keep your unique passwords secure and will allow you to reference them easily.
* Enable Multi-Factor Authentication on password managers and accounts whenever possible.
* Never store passwords in text files, spreadsheets, or documents on your computer.

Physical Security

# Physical Security in the Workplace

## Unattended workstations

* Always lock your workstations while they are unattended
* An unlocked workstation allows complete access to any who passes by. Leaving your workstation unlocked can cause theft of sensitive information or allow someone to install malware on your machine.
* Lock your windows machine by pressing the Windows key + L

## confidential Physical documents

* Confidential documents in the workplace should be treated with the same security as documents on your computer.
* Use secure shred bins for disposing of sensitive paper documents and electronic media.
* Lock away confidential documents at the end of the work day or when they are unattended

## Tailgating/Impersonation

Using someone else to gain access to a building by following them into unauthorized areas, or pretending to be with a vendor, company, client, etc. to coax employees to believe that you belong in the facilities.

* Have a policy in place for visitors. (visitor badge, check-in system, etc.)
* Don’t be afraid to ask who someone is and why they are there.

## Shoulder Surfing

Shoulder Surfing is the act of direct observation, such as looking over someone’s shoulder to obtain information.

* Don’t view potentially sensitive information in public areas like Airports, Coffee Shops, Flights
* Curiosity, espionage, and competitive advantage can give an incentive to shoulder surf
* Invest in a privacy filter if you are constantly working with sensitive information