



throttle.net.com

TODAY'S PRESENTER:

Chris Montgomery

Director of Sales



throttlenet.com



WHY ARE WE HAVING THIS DISCUSSION?

RANSOMWARE ATTACKS ARE ON THE RISE

- Globally, there were 304.7 million ransomware attacks in the first half of 2021, a 151% increase since 2020. (SonicWall)
- The most common tactics hackers use to carry out ransomware attacks are email phishing campaigns, RDP and software vulnerabilities. (Cybersecurity & Infrastructure Security Agency, 2021)



SO ARE THE COSTS OF A RANSOMWARE ATTACK



- The average ransom payment was \$139,739 in Q3 of 2021, up 2.3% from Q2 of 2021. (Coveware)
- 32% of ransomware victims paid the ransom in 2021. (Cloudwards)
- Of the 32% of ransomware victims who paid the ransom in 2021, only 65% of their data was ultimately recovered. (Cloudwards)

AND ITS ONLY GOING TO INCREASE

- Ransomware will cost victims over \$265 billion annually by 2031
- By 2031, a ransomware attack will occur every 2 seconds – up from every 11 seconds in 2021
- By 2025, 30% of all governing bodies will enact legislation to combat ransomware



AGENDA

- **How to Safely Use the Internet**
- **How to Identify Attacks when Using Email**
- **The Importance of a Secure Connection**
- **The Pitfalls of Using a Company Device for Personal Use**
- **Best Practices if you Must Use a Company Device**
- **Who We Are and A Special Offer from ThrottleNet!**

HOW TO SAFELY USE THE INTERNET

HTTPS keeps your information secure!

Look for 'HTTPS' in the web address you're viewing.

Secure websites will have a padlock icon in the browser's address bar that can be clicked on for more information regarding that security of that site



Look for this symbol to ensure that you're on a secure site.

VARY PASSWORDS

Password reuse is still a common practice



52%

reuse the same password for multiple (but not all) accounts

35%

Use a different password for all accounts

13%

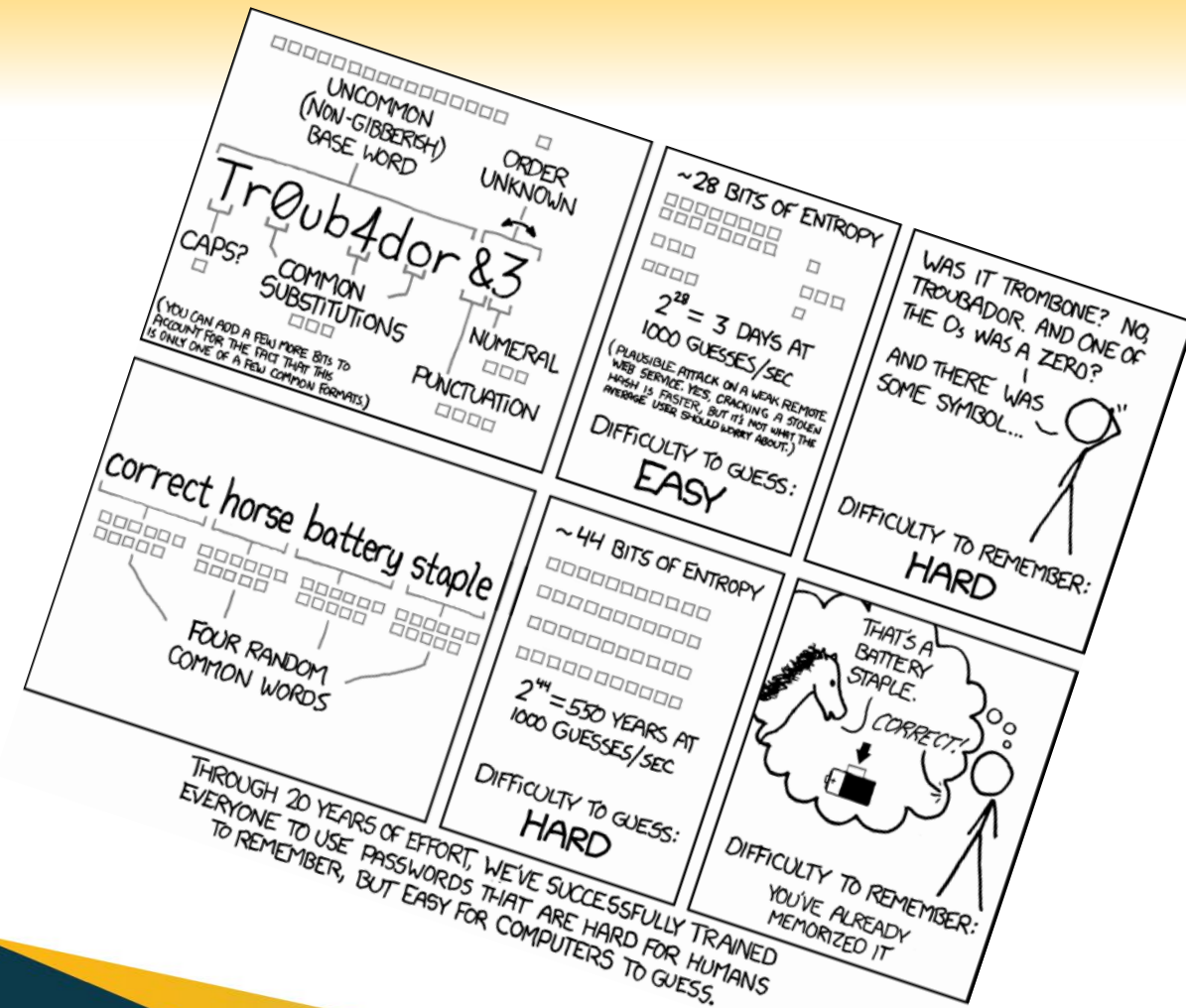
Reuse the same password for all their accounts

When you use the same password across many sites it makes it easy for criminals to hack all your accounts.

Use more complex and varied passwords for sites with personal information such as banking and healthcare sites.

BE CREATIVE WITH PASSWORDS

Tr0ub4dor&3 could take just (3) three days to crack, according to verified security researchers, while *CorrectHorseBatteryStaple* could take 550 years to crack*



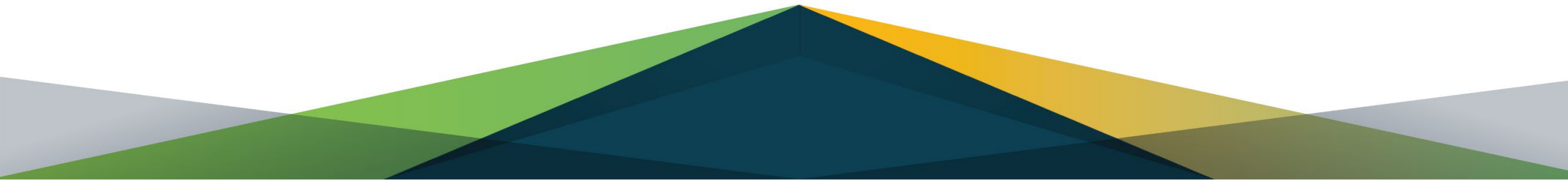
PASSPHRASE VS. PASSWORD

WHAT IS THE DIFFERENCE

Creating a complex password is not as difficult as you might think. Just think of it as a passphrase instead. Some tips to create an effective passphrase include:

- **Using your favorite movie line quote that is at least sixteen (16) characters in length**
- **Use a lyric from your favorite song**
- **Affirmational statements to get your day started on a positive note**

*Did you know it would take **16 billion times longer** to crack a 16-character password compared to an 8-character password?*



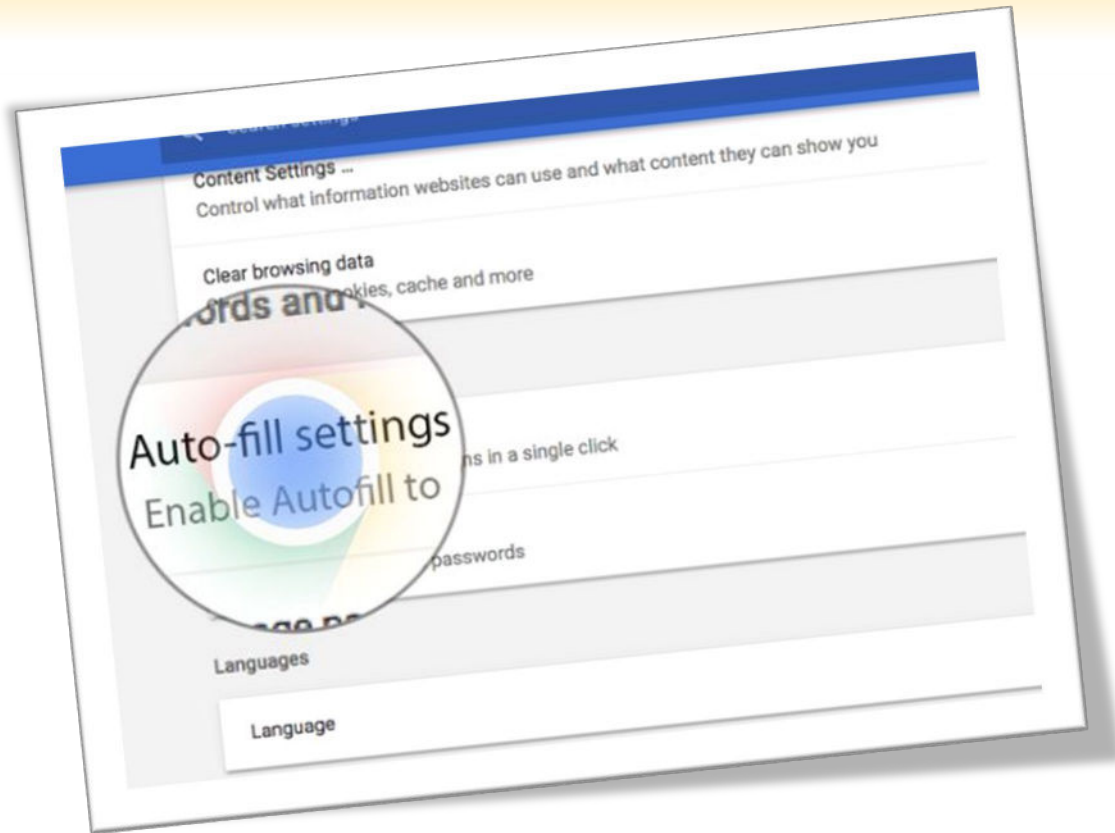
IS MULTIFACTOR AUTHENTICATION (MFA) THE SOLUTION?

MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account.

- Remote work makes MFA a critical part of network security
- MFA is effective in preventing most compromises



DON'T USE AUTOFILL



If needed, use a third-party application like LastPass to help you remember passwords.

AutoFill / Auto Complete / Remember Me – these can all cache your private data locally on your computer which can make it accessible to anyone that uses that computer.

DON'T CLICK IT

Ignore pop ups that claim your computer is infected. Rogue scanners are a category of scam software sometimes referred to as "scareware".

Rogue scanners masquerade as antivirus, antispyware, or other security software, claiming the user's system is infected in order to trick them into paying for a full version.

Avoiding infection is easy - don't fall for the bogus claims.

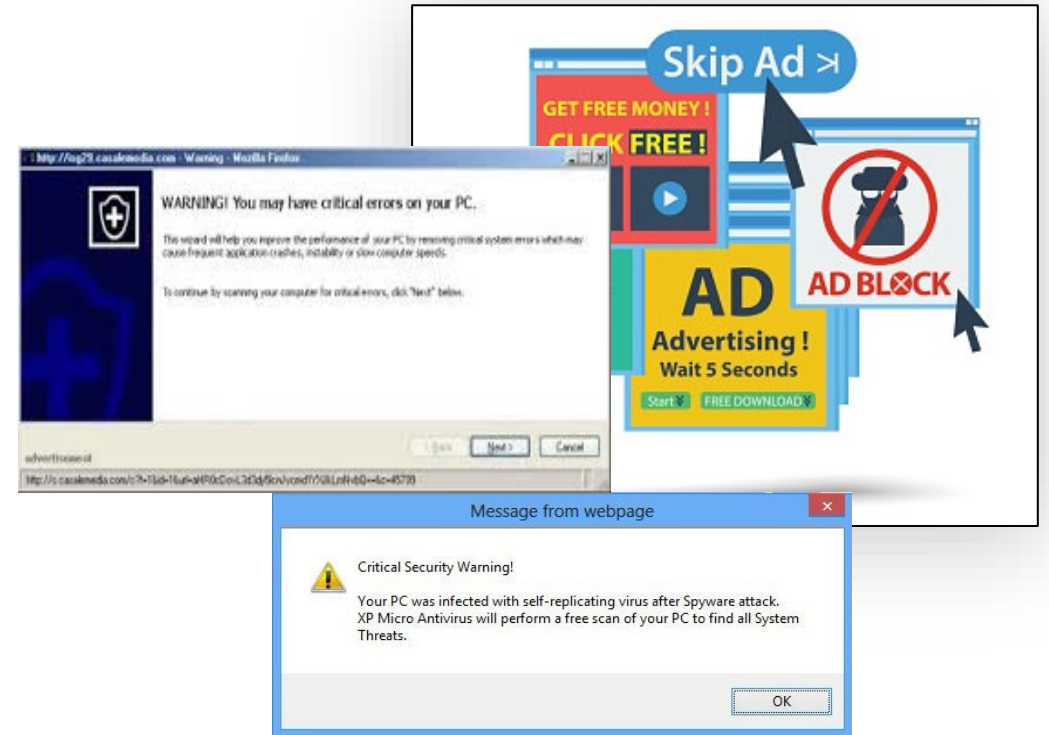


DON'T RUN IT

Beware of windows or pages that prompt you to click a link to run software.

Malicious websites can create prompts that look like messages from your browser or computer.

If you see a pop-up you think is risky, go to the company's website for scans and downloads.



BROWSER ADS



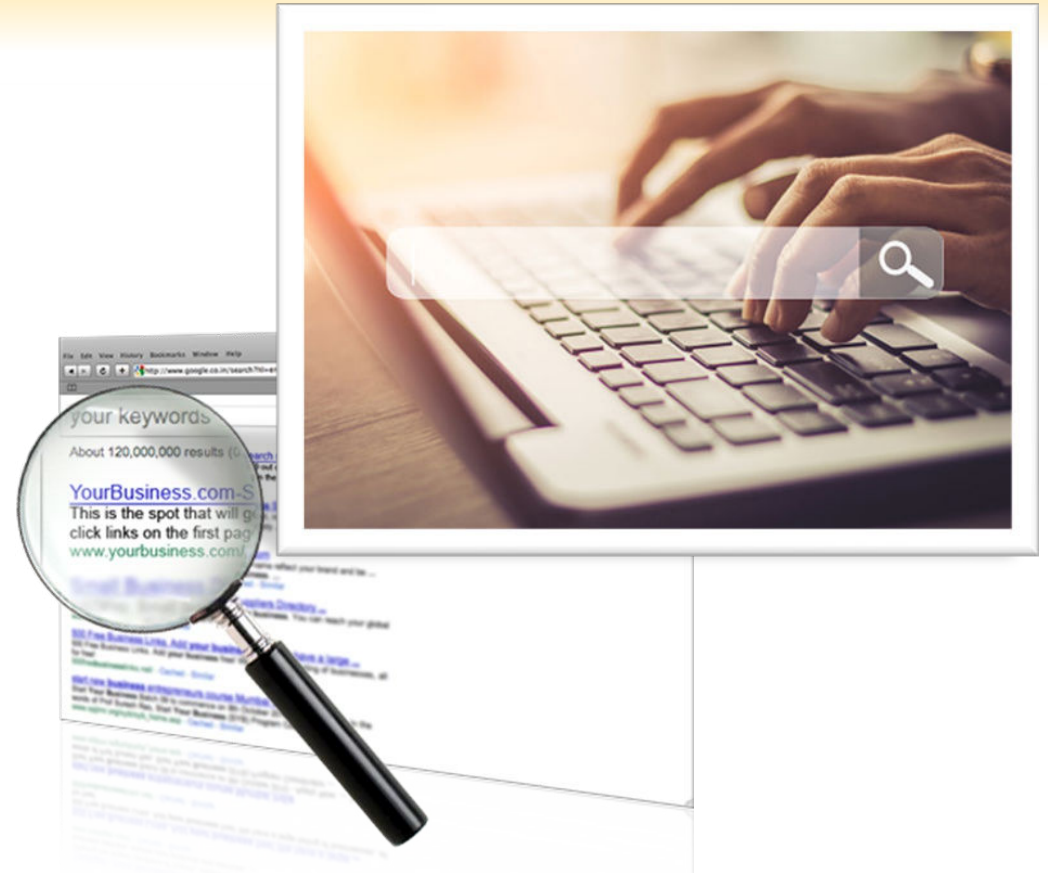
Some advertisements encountered online are nefarious and can be used to compromise your security.

Consider installing an add-on or extension to block web advertising such as uBlock Origin or Adblock Plus.



OTHER TIPS

- **When you use a search engine be very careful of the result you click on.** Hackers use legitimate looking topics to trick you into clicking. Scrutinize the URL to ensure you are going to a legitimate web site.
- **Watch for shortened URLs, and numbers, hyphens or special characters in a URL.** Scammers manipulate URLs to trick users. Be wary of URL's posted in Facebook and sent via email. Use a search engine to identify the actual URL.





HOW TO IDENTIFY ATTACKS WHEN USING EMAIL

What is Social Engineering?

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.



What is a phishing attack?



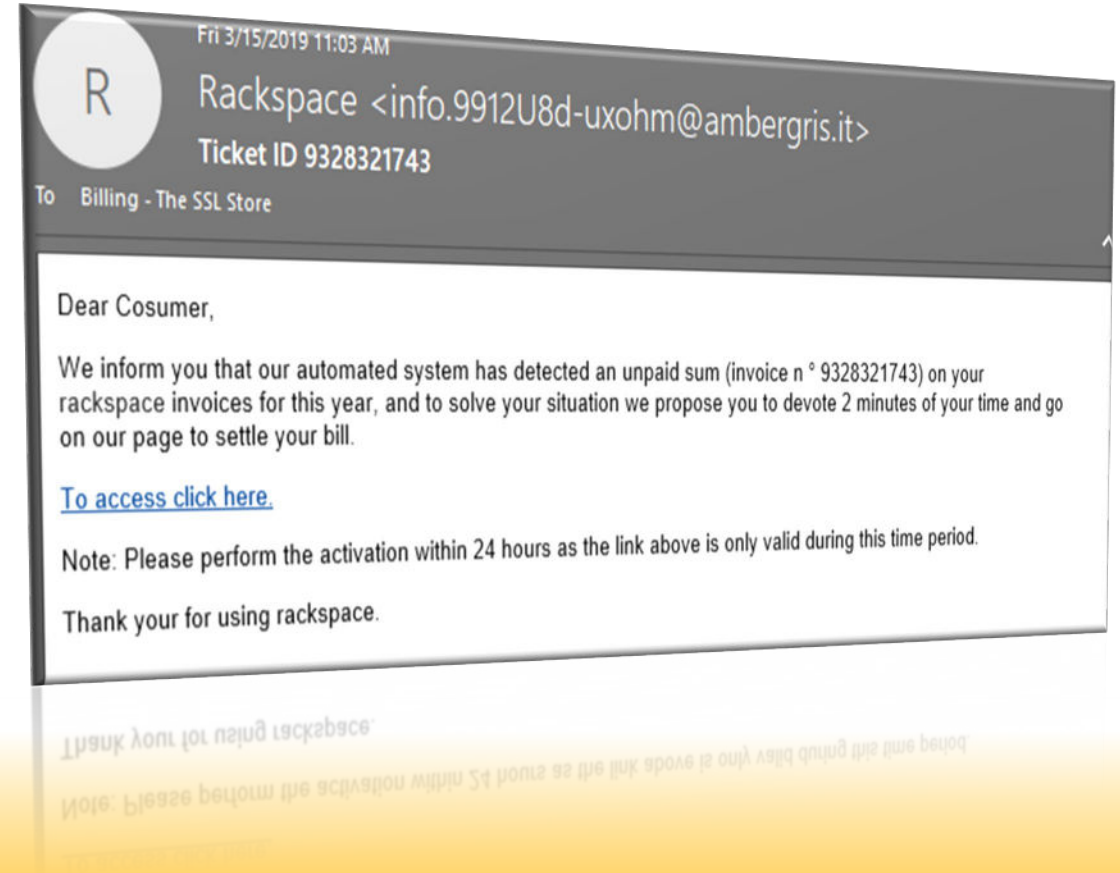
Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

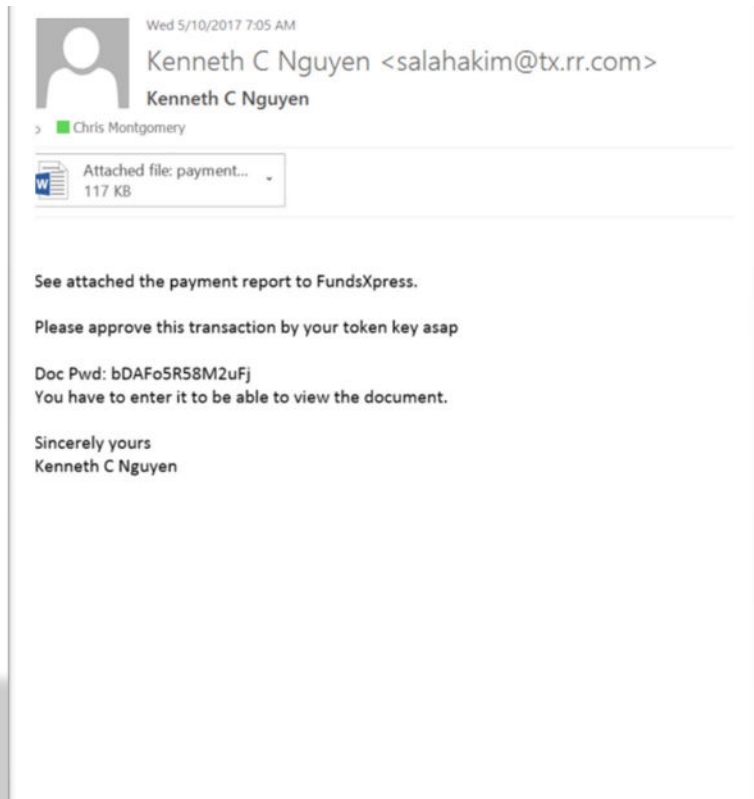
It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

How to identify a Phishing attack:

- "From" address is odd
- Unprofessional punctuation
- Errors in grammar, capitalization & punctuation
- Links to an external website
- Use of threat to promote immediate action





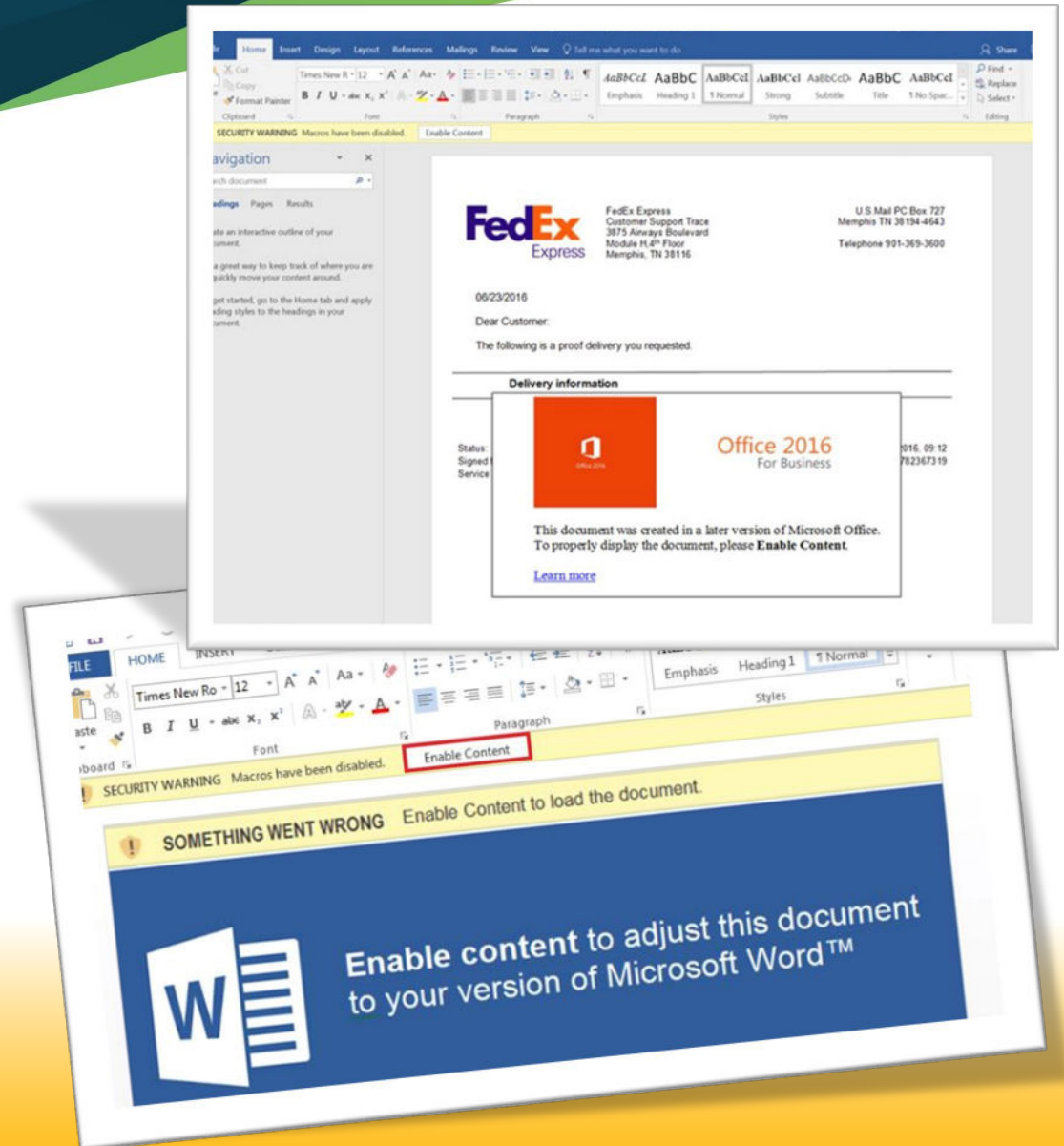
Example #1:

Phishing Attack with attachment in email Inbox



Example #2:

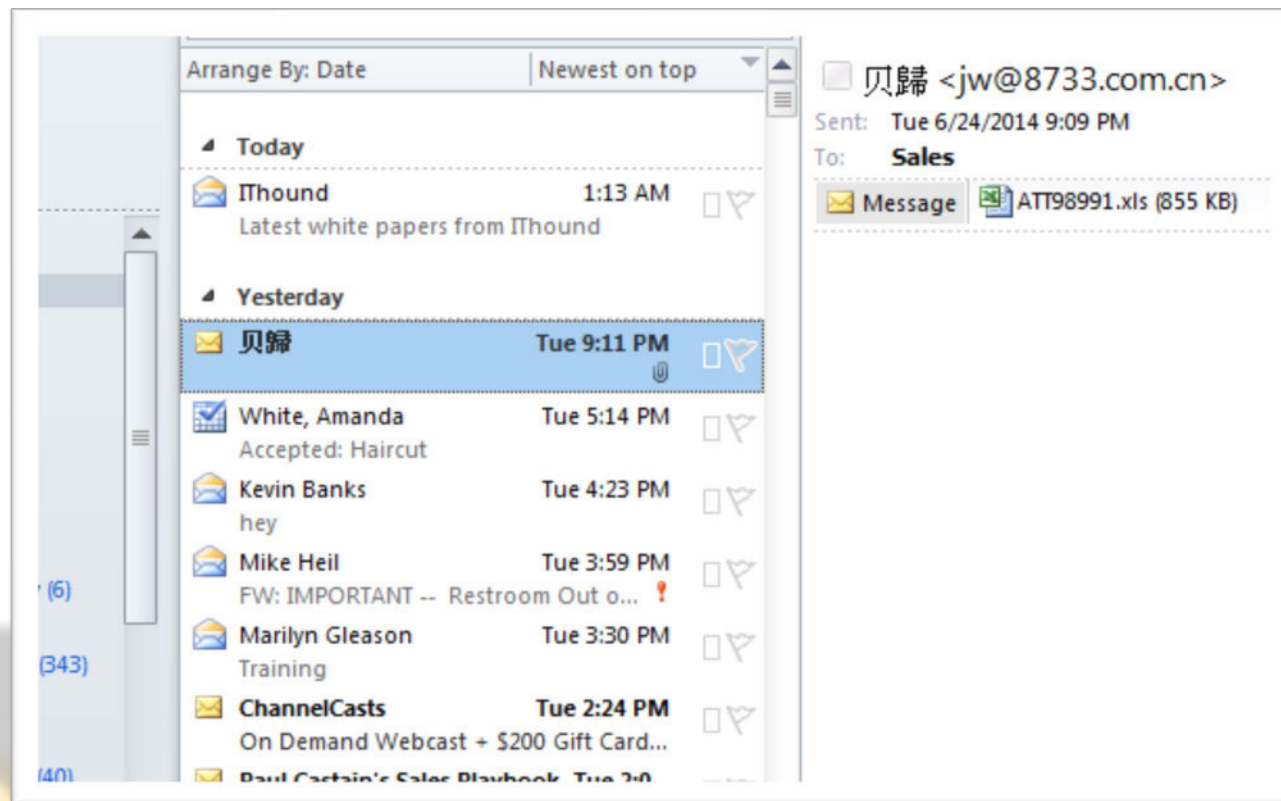
Phishing Attack from trusted source such as FedEx, Amazon, USPS or UPS





Example #3:

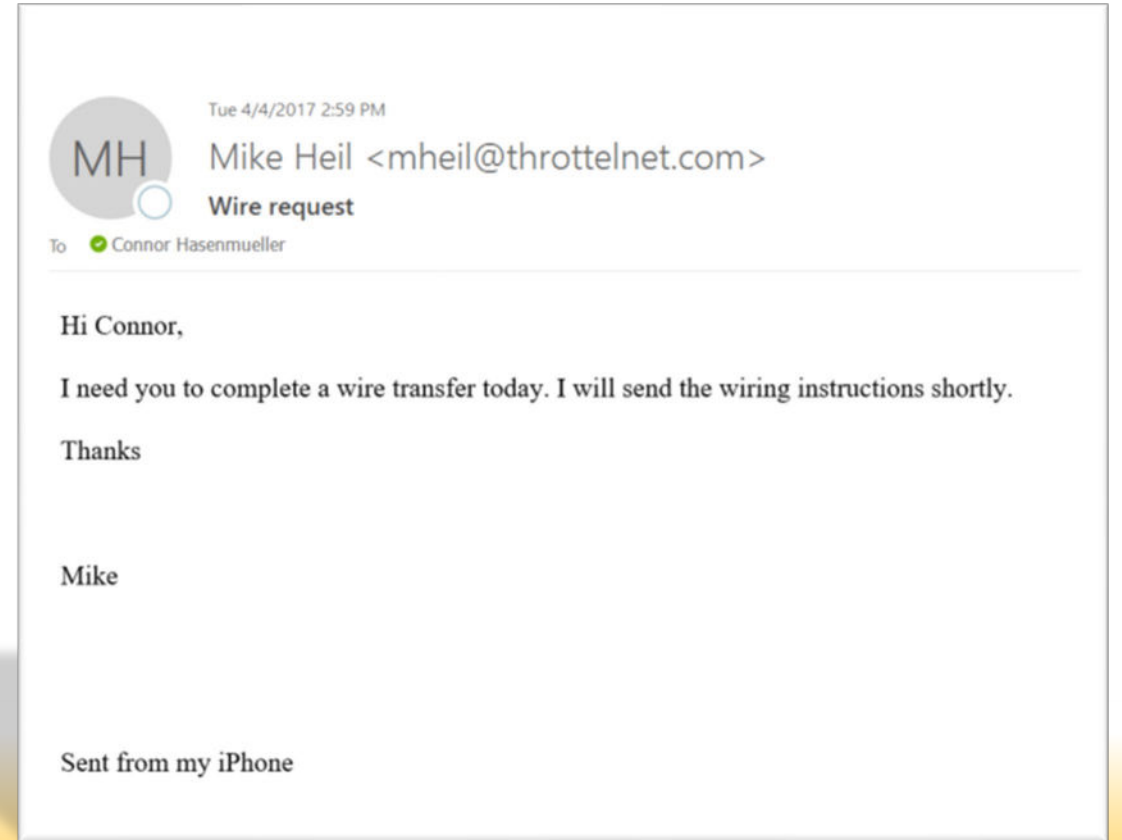
Phishing Attack from
overseas with
attachment in email Inbox





Example #4:

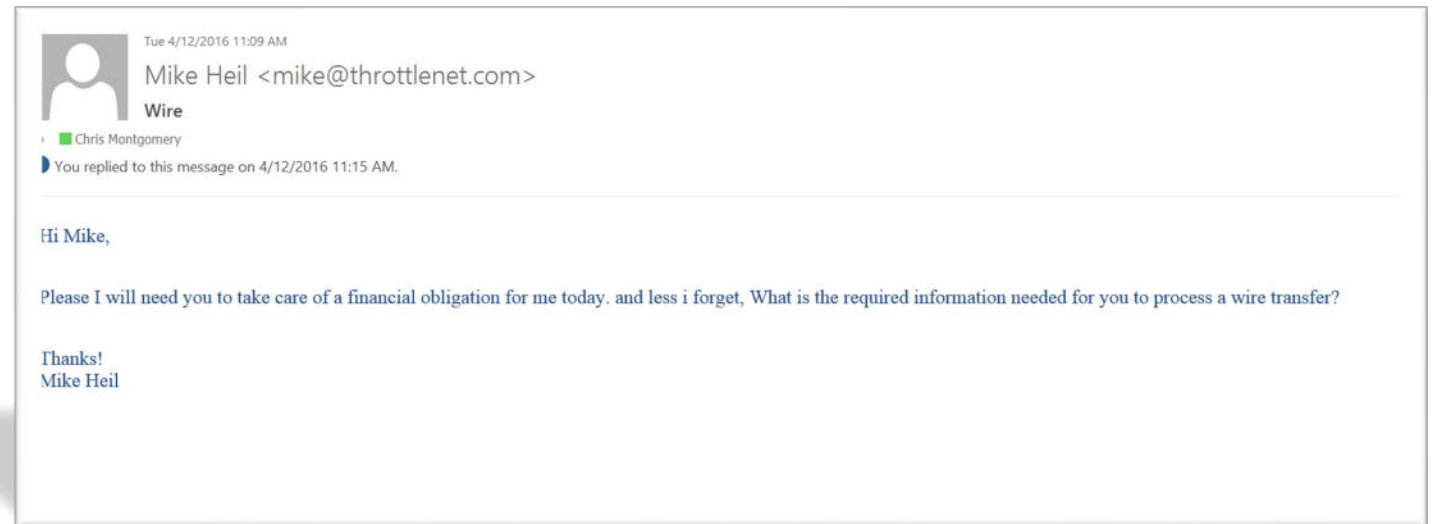
Phishing Attack with a wire transfer or gift card request





Example #5:

**Phishing Attack with
Attempt to gain
information**



IGNORE UNSOLICITED LINKS IN EMAILS

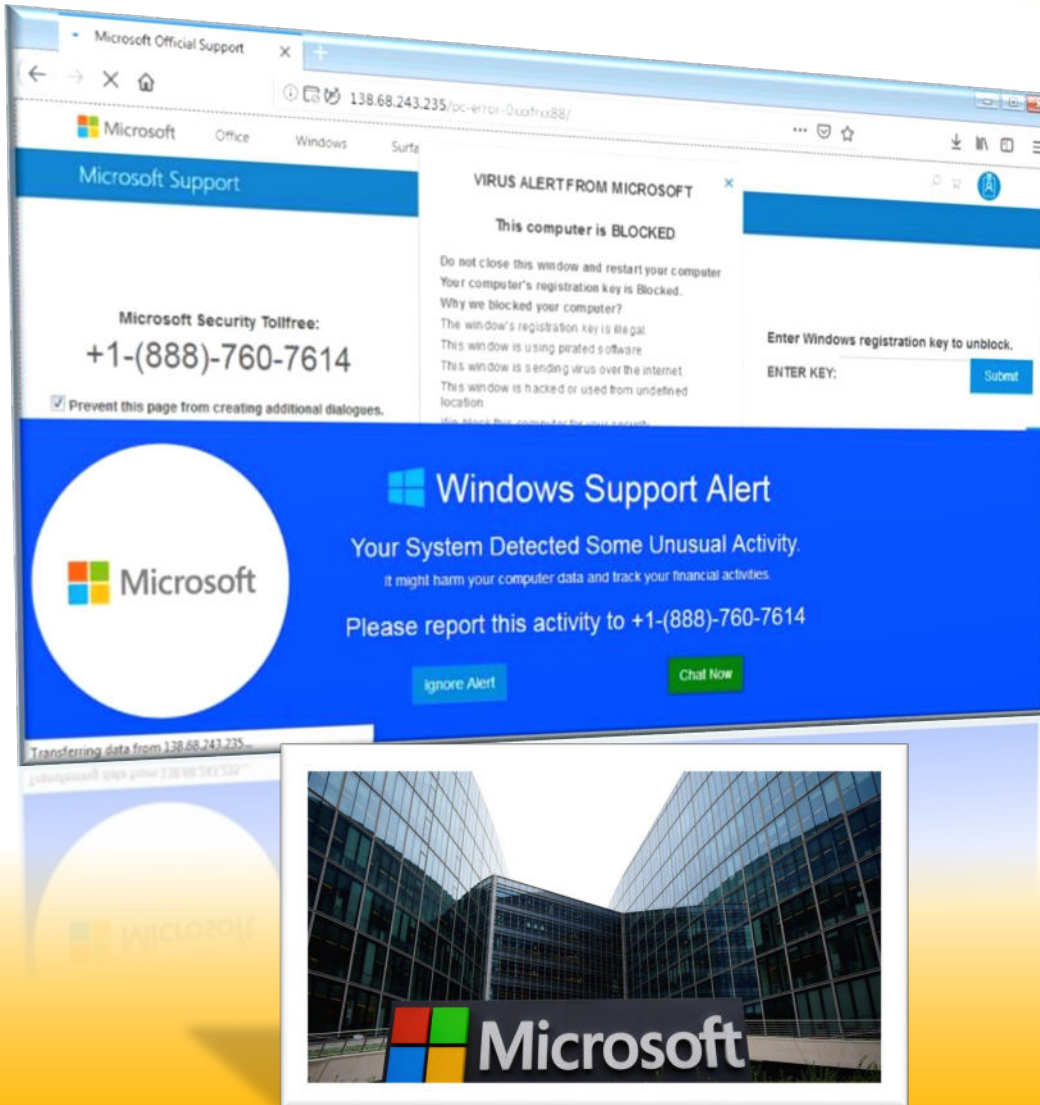
- Malicious or fraudulent links in email and IM are a significant vector for both malware and social engineering attacks
- Reading email in plain text can help identify potentially malicious or fraudulent links




DON'T FALL FOR IT

If a person calls and says he's from Microsoft Support and wants to connect to your PC, says your PC is infected or sending email on its own....

HANG UP



SECURE WEB BROWSING CHECKLIST

- **DO NOT TRUST** your browser to protect you
- **CHECK** security and privacy settings by clicking on the top right corner of your respective browser
- **CHECK** for the secure symbol  next to the URL to ensure it is secure
- **NEVER** give out personal information to receive something for "free" online (home address, telephone number, email address)
- **DIFFERENTIATE** passwords from site to site and use complex passwords containing at least one of the following:
 - Capital letter
 - Symbol
 - Use a "passphrase" or key stroke pattern
- **BEWARE** of pop-ups or websites that prompt you to run computer software (antivirus, antispyware or other security software)
- **BE CAUTIOUS** on downloading files.
- **WATCH** for shortened URLs, numbers, hyphens or special characters
- **NEVER** trust "free" content
- **BE CAUTIOUS** of auto-complete for forms or "remember my password" on frequently accessed websites



12970 Maurer Industrial Dr., Suite 150
St. Louis, MO 63127
866.826.5999

DON'T BECOME PHISH BAIT

It's easier than you think.

HOW TO SPOT PHISHING
- spelling
- a sense of urgency
- links that don't make sense
- odd grammar
- unusual requests

 **throttle**
ThrottleNet.com/PhishBait

15 WAYS TO PROTECT YOUR BUSINESS FROM CYBERATTACKS!

SECURITY AWARENESS TRAINING

ThrottleNet knows your users are your first line of defense and your weakest link. That's why we provide solutions to teach them about data security, email phishing attacks, and social engineering via best-in-class web-based training solutions.

ADVANCED ENDPOINT DETECTION & RESPONSE

ThrottleNet protects your data from malware, viruses and cyberattacks with advanced, next-generation endpoint security solutions. This protects your network using the power of AI (Artificial Intelligence), as well as the backing of a 24/7 Security Operations Center (SOC).

EMAIL BACKUP VIA DATTO

A common misconception is that Microsoft is liable for and/or backs up any data stored in Microsoft 365. However, this could not be further from the truth. ThrottleNet ensures your data in Microsoft 365 is backed up 3X daily via a best-in-class business continuity and disaster recovery provider - Datto.

COMPUTER UPDATES

ThrottleNet keeps your 3rd applications and Microsoft operating system updated and patched with the most current security updates via automation to protect against the latest known attacks and vulnerabilities.

MICROSOFT OFFICE PROTECT FOR MS365

Email is the target of most attacks which is why ThrottleNet includes Microsoft Office Protect. This solution monitors for suspicious sign-in behavior, administrator abuse, odd mailbox activities and more.

PASSWORDS

ThrottleNet applies security policies including the requirement for complex passwords as well as password refresh policies ensuring passwords are changed regularly.

ENTERPRISE EMAIL PROTECTION

ThrottleNet secures your email since most attacks originate here. Our solution is designed to reduce spam and includes the capability of sending secure, encrypted email when requested. ThrottleNet ensures your data is protected while at rest or in motion by turning on encryption within your server and data storage solutions.

DARK WEB RESEARCH

ThrottleNet performs regular scans of the Dark Web to provide real-time reports on what passwords and accounts have been compromised allowing you to be proactive in preventing a data breach.

SECURE EMAIL CHECKLIST

- **DON'T OPEN** suspicious links
- address looks suspicious or odd
- punctuation is used in the email (!!!!)
- grammatical errors (capitalization and punctuation)
- links
- language to provoke immediate response
- unexpected (突然) foreign characters /
- IM that are unexpected -
- suspicious via links received in an email
- bookmarked or a well known URL
- without verifying in
- requests from sender
- spyware you do so
- section



THE IMPORTANCE OF A SECURE CONNECTION



UNSECURED WI-FI AND THE DANGER OF IGNORANCE

According to a survey of 1,025 people conducted by Symantec

- **60% of American consumers believe that their information is safe when using public Wi-Fi**
- **50% believe that they bear any personal responsibility for ensuring that their data is secure.**
- **17% of those surveyed believe that individual websites are responsible for making sure that visitor data is secure, while the same percentage think that this duty falls to the Wi-Fi network provider.**



PUBLIC WI-FI IS NOT SECURE

When you sign on to public Wi-Fi, you may also be sharing your data with the companies providing the Wi-Fi. Many public Wi-Fi networks such as in airports and hotels will also prompt you to install a “digital certificate” to use their internet. They may do this to scan your traffic for malware — but this also allows them to read your traffic, even if it’s to a site using https (which encrypts information).

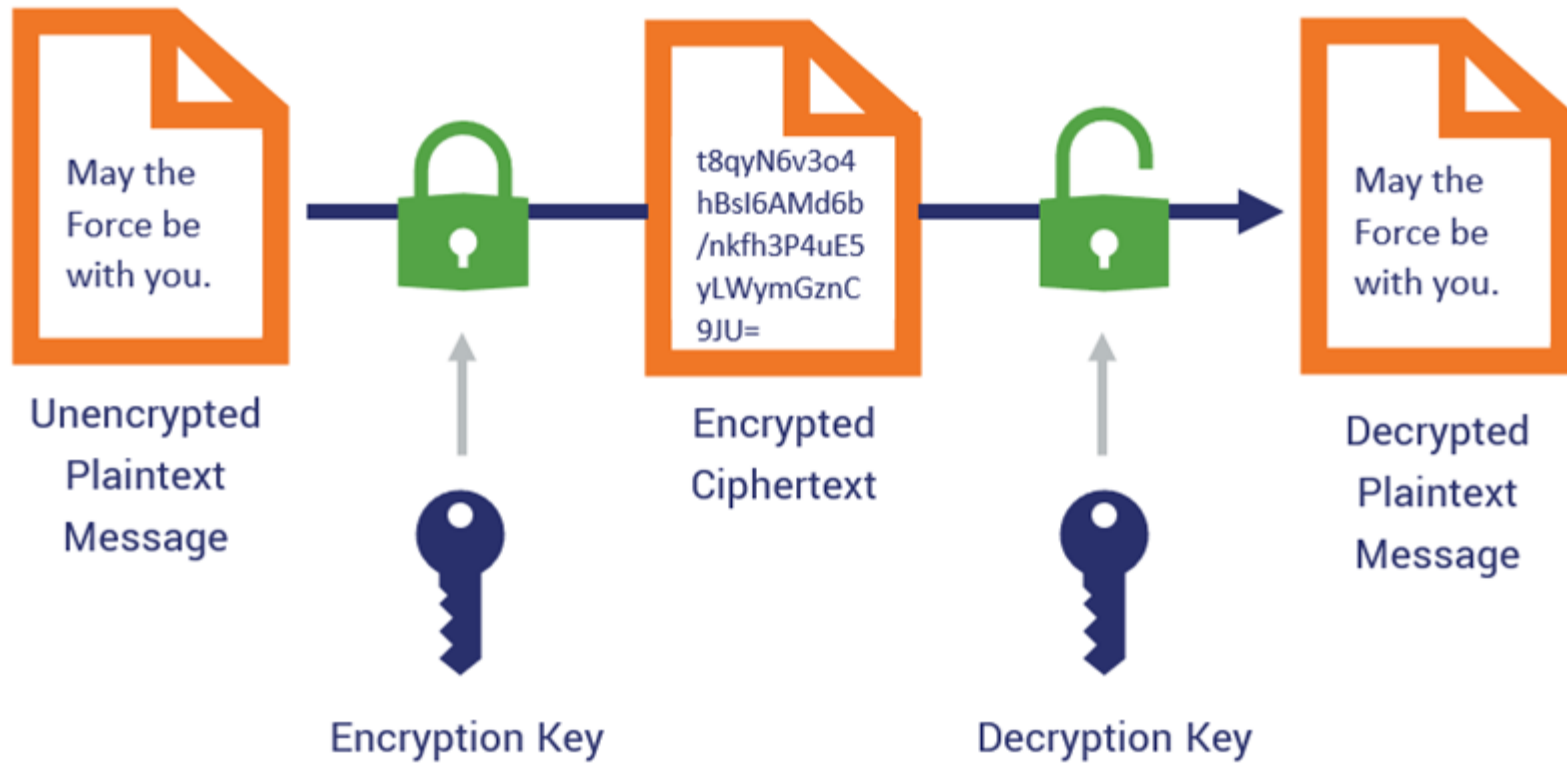


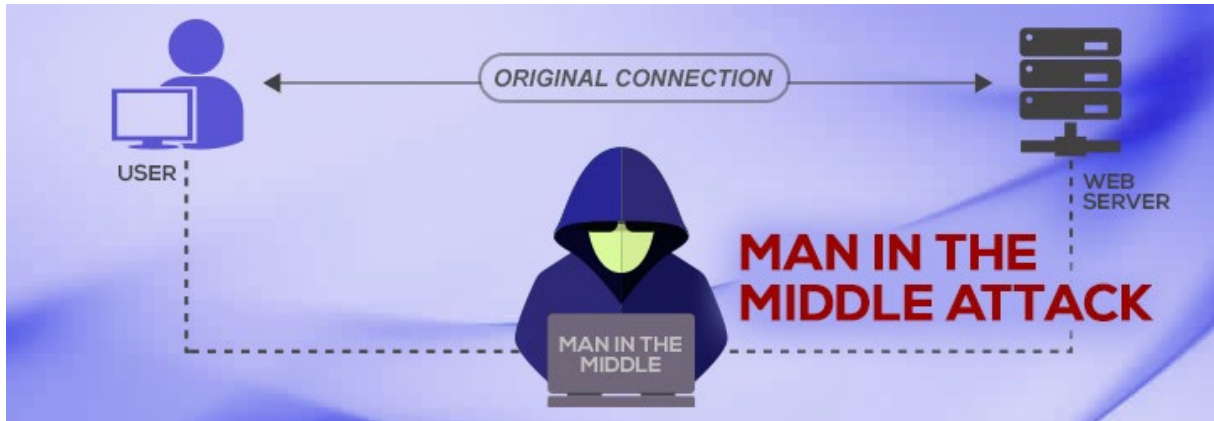
WHAT'S THE DIFFERENCE BETWEEN A SECURE AND UNSECURE WIFI CONNECTION?

A secure connection is one that's fully encrypted; meaning as data is transferred, anyone that might access said data will only see a mishmash of numbers and letters

An unsecure connection allows bad actors to see exactly what the data is- in its raw form - which is how they are able to steal said data.

How Encryption Works





MAN IN THE MIDDLE ATTACKS

A “Man in the Middle” attack is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.



WI-FI HONEYPOTS

When cybercriminals setup a fake wireless hotspot, this is known as a Wi-Fi “honeypot”.

It’s designed to trap unsuspecting visitors within a specific location.

The fake hotspot may look just like what you’d expect – down to the name and logo of the establishment.



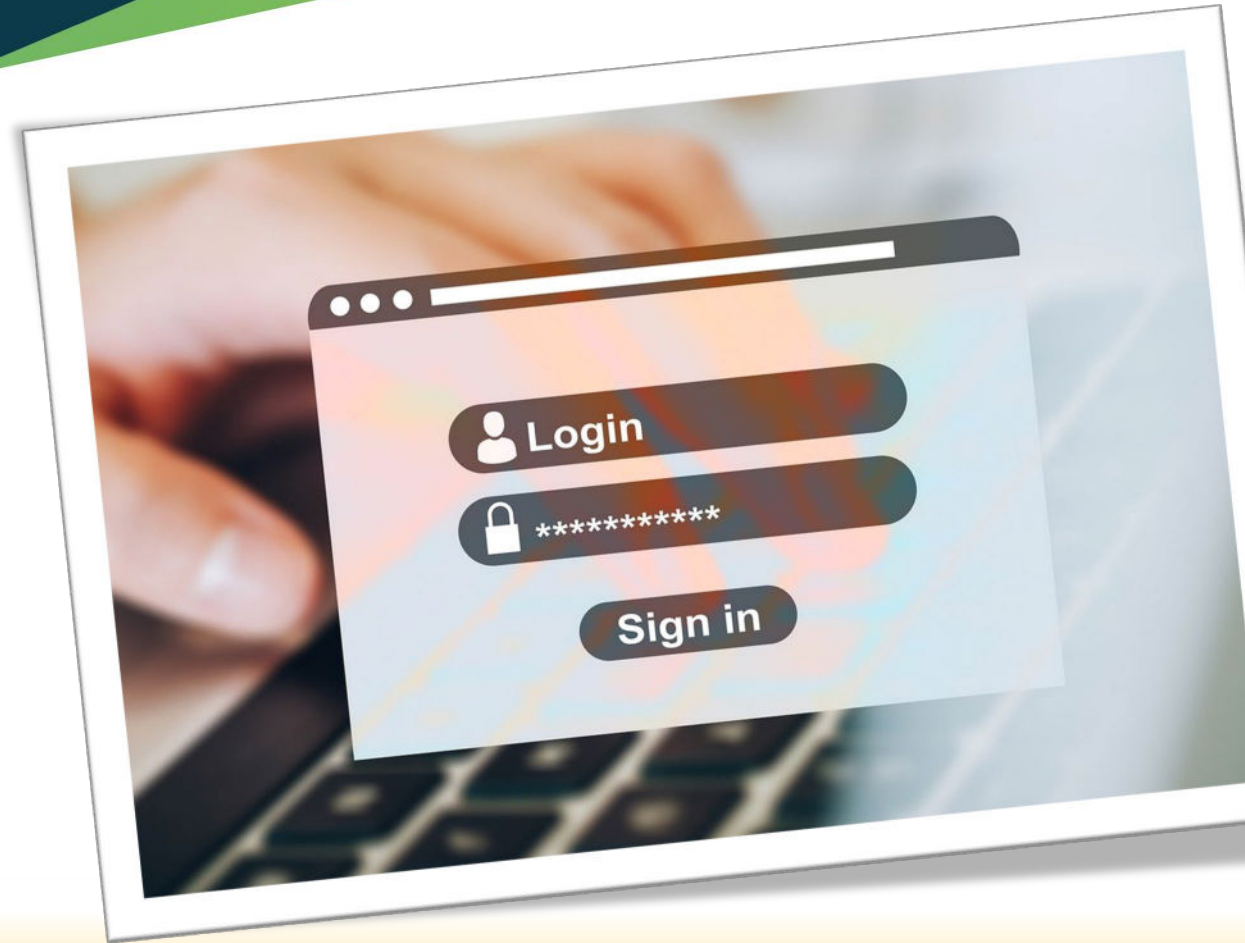
Data Loss

Using an unsecure connection could allow your data to be exposed to bad actors and, in turn, shared or sold on the Dark Web.

INTERCEPTING YOUR LOGIN CREDENTIALS

Hackers nearby can eavesdrop on your connection to gather useful information from your activities.

Data transmitted in an unencrypted form (i.e., as plain text) may be intercepted and read by hackers with the correct knowledge and equipment.



THE PITFALLS OF USING A COMPANY DEVICE FOR PERSONAL USE



WHO IS USING THEIR WORK PC FOR PERSONAL USE?

A survey conducted by antivirus vendor Malwarebytes asked respondents how they used their work devices. The company found that....

- 53% reported sending or receiving personal email
- 52% read news
- 38% shopped online
- 25% accessed their social media
- 22% downloaded or installed non-company software.



IF THE DEVICE IS BROKEN, IT COULD BE YOUR RESPONSIBILITY TO REPLACE IT

In addition, your IT Department may remotely wipe the machines; meaning, even if it turns up later, the data within could already be gone and unrecoverable.

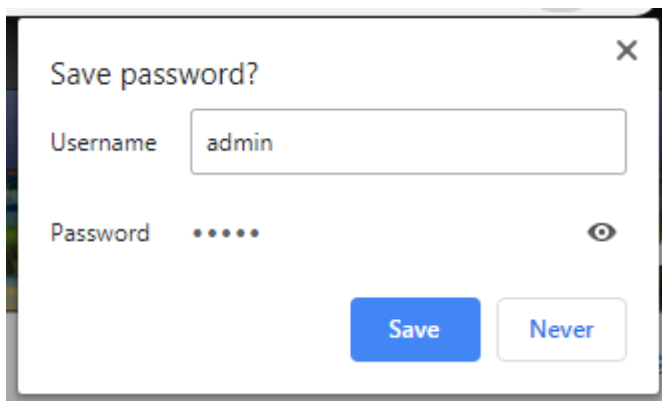
YOUR EMPLOYER COULD BE WATCHING YOU

More employers are monitoring activity on corporate devices as more employees work from home due to the COVID-19 pandemic.

Research from Skillcast and YouGov that shows one in five companies (20%) are "using technology capable of tracking workers' online activity or have plans to do so in the future."



BEST PRACTICES IF YOU HAVE TO USE YOUR WORK PC FOR PERSONAL USE



DON'T: SAVE PERSONAL INFORMATION ON A WORK DEVICE

According to the Society of Human Resource Management (SHRM) many organizations have a clause in their computer, email and internet use policy that makes storing personal passwords a potentially precarious move.

"E-mail and other electronic communications transmitted by [Company Name] equipment, systems and networks are not private or confidential, and they are the property of the company. Therefore, [Company Name] reserves the right to examine, monitor and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite."



DON'T: MAKE OFF-COLOR JOKES ON MESSAGING SOFTWARE.

As chatrooms like Slack, Campfire and Google Hangout become increasingly handy for team collaboration, it's easy to use them as though you were in the office break room having a gossip session with a colleague while raiding the fridge. However, those messages are being kept on a server somewhere and are just as retrievable as emails.



DON'T: ACCESS FREE PUBLIC WI-FI WHILE WORKING ON SENSITIVE MATERIAL.

With so many of us working remotely or sending a few work emails over the weekend from a cafe, it's tempting to grab your laptop and log on to free public wi-fi.

However, places that offer free wi-fi like the neighborhood coffee shop, the airport or the hotel, can open you up to fraud.



**DON'T:
ALLOW FRIENDS OR NON-IT
DEPARTMENT COLLEAGUES TO
ACCESS YOUR WORK COMPUTER.**



DON'T: STORE PERSONAL DATA.

It's so easy to have a "personal" folder on your desktop full of all the cute photos your spouse sent of your children or to save that receipt from the plumber, but it's important to remember that a work device is not your property—it belongs to the company.



DON'T: WORK ON YOUR SIDE HUSTLE WHILE AT THE OFFICE.

Many of us have second or third jobs that we do as hobbies or to earn extra cash , but don't blur the lines while you're "on the company dime."

ABOUT THROTTLENET AND A SPECIAL OFFER



throttnet.com



WHAT DO WE DO?

ThrottleNet provides IT Support, Service and Cybersecurity solutions to businesses of all industry types and sizes.

Our average client size is roughly thirty (30) users and/or PC's, but we service clients as small as five (5) and as large as five hundred (500)+



WHO DO WE SERVE?

ThrottleNet services all industry types specializing in cybersecurity and general IT support.

We serve over 155 clients throughout Missouri and the United States from our national headquarters in Sunset Hills, MO

STOP BY OUR BOOTH

- Register to win a FREE drone!
- Get a FREE Dark Web scan
- FREE bag o'shwag full of cybersecurity gear

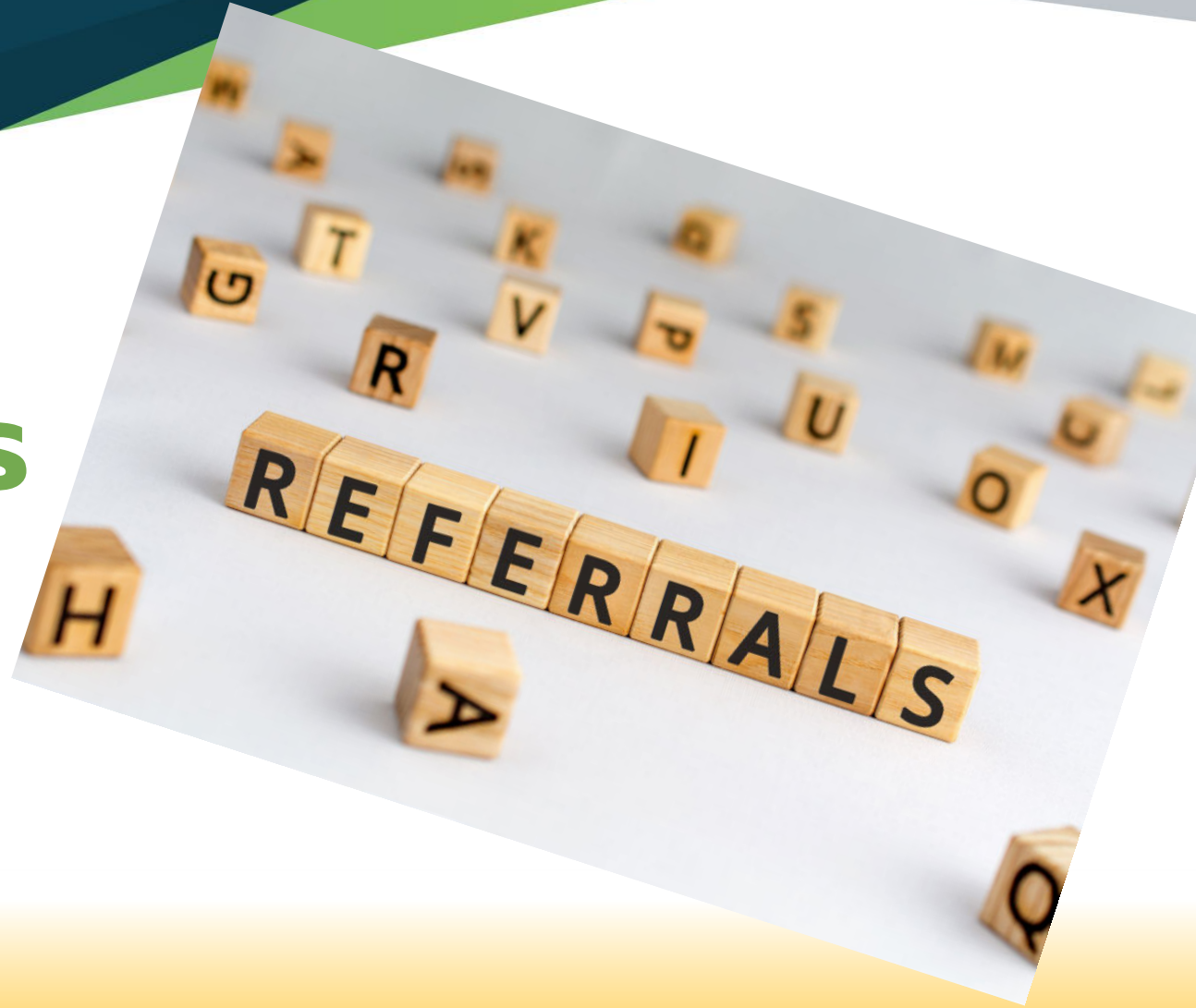


ThrottleNet Loves Referrals

11+ Users/Workstations = \$1000

10 Users/Workstations or less = \$500

<https://www.throttpnet.com/why-throttpnet/referral-program/>



WANT A COPY OF THIS PRESENTATION?



Click on the link below www.throttlenet.com/MACA

For more information on
ThrottleNet visit us online at
throttlenet.com or call us toll free
at 866-826-5966



throttlenet.com



throttlenet



throttlenet.com