



throttlenet.com

CYBERSECURITY AWARENESS TRAINING 2021



[throttlenet.com](https://www.throttlenet.com)







TODAY'S PRESENTER:

Chris Montgomery

Director of Sales



AGENDA

-  The State of Cybersecurity 2021
-  The Most Common Types of Cyber Attacks
-  Security Definitions
-  General Best Practices
-  How to Safely Browse the Internet
-  How to Securely Use Email

THE STATE OF CYBERSECURITY



throttnet.com



**In 2020 A New Ransomware Attack
Occurred Every
14 Seconds**

(2021, it will be every 11 seconds)

\$10.2 BILLION

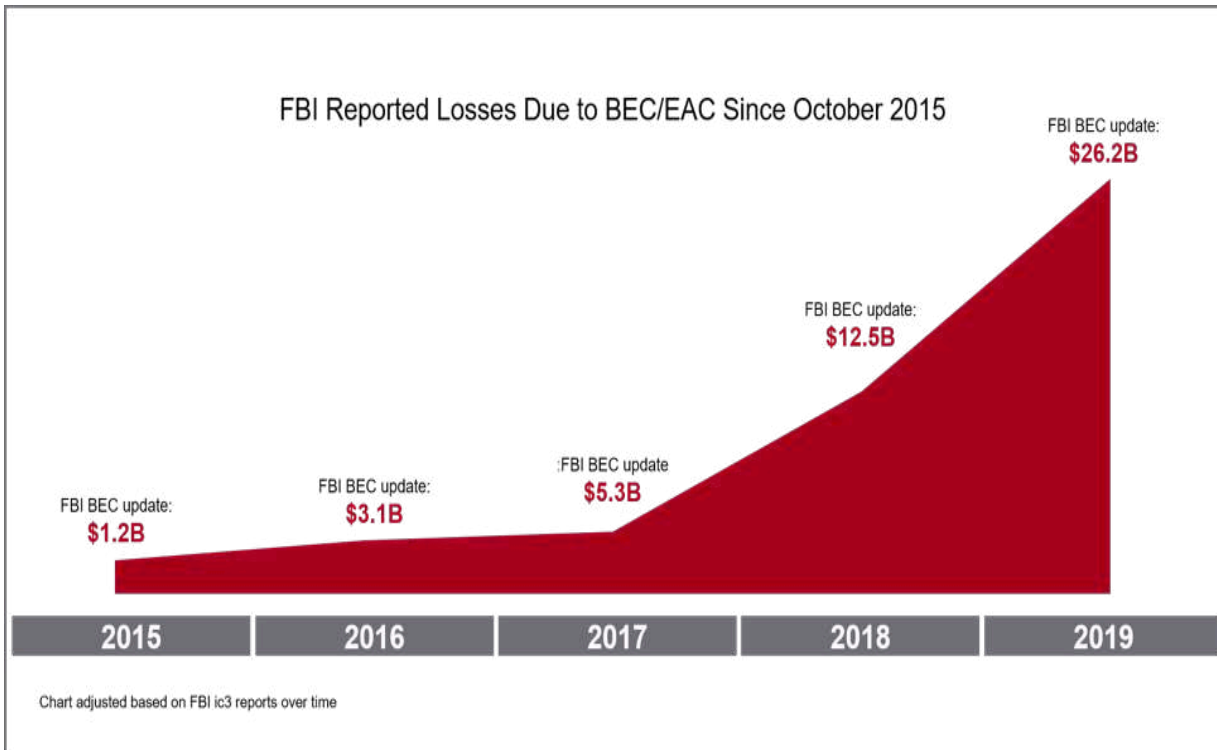
IN VICTIM LOSSES *REPORTED*

The Internet Crime Complaint Center (IC3) routinely analyzes complaints submitted by victims of internet crimes. It emphasizes the IC3's efforts in monitoring trending scams such as Business Email Compromise (BEC), Ransomware, Tech Support Fraud, and Extortion.

Corporate Data Breach \$53,398,278	Personal Data Breach \$120,102,521	Credit Card Fraud \$111,491,163
Business Email Account \$1,776,549,688	Identity Theft \$160,305,789	Investment Fraud \$222,186,195



BUSINESS EMAIL COMPROMISE



Two common financial losses related to BEC:

- 1) Fraudulent transfers of money
- 2) Obtaining personally identifiable information of staff to use in future attacks

INDUSTRIES CONSISTENTLY UNDER ATTACK

Finance



Healthcare



Construction



Legal



Manufacturing

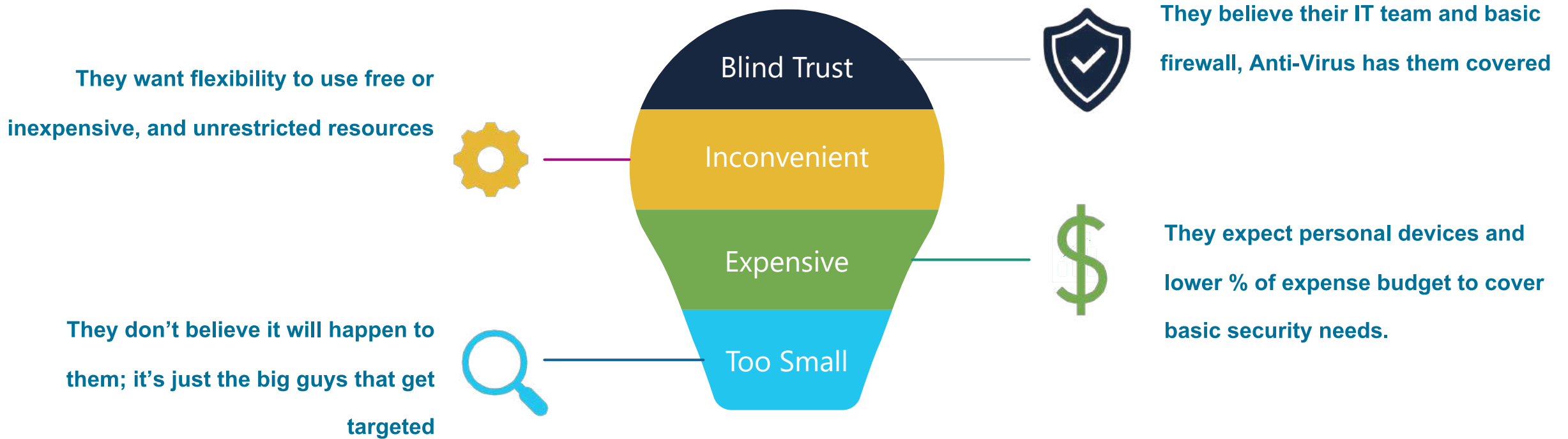




WHY DON'T WE HEAR ABOUT SMB CYBER ATTACKS?

- **Not Newsworthy**
- **Extremely Embarrassing to admit**
- **Horrible PR:**
Do you want clients to know?
- **Legal Ramifications:**
Many incidents go unreported

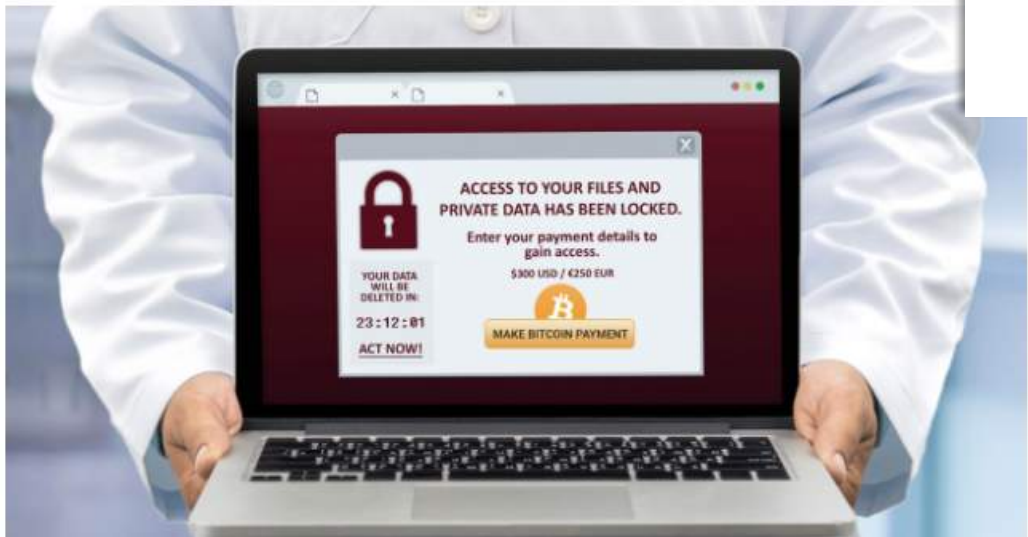
SMB CHALLENGES WITH CYBERSECURITY





46% of SMBs have been targeted by ransomware, 73% have paid the ransom

Ransomware attacks are not at all unusual in the SMB community, as 46% of these businesses have been victims. And 73% of those SMBs that have been targets of ransomware attacks actually have paid a ransom, Infracore reveals.



SMALL BUSINESS PLAYBOOK

Cyberattacks now cost small companies \$200,000 on average, putting many out of business

PUBLISHED SUN, OCT 13 2019-10:30 AM EDT

<https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>

LAW FIRM / PROFESSIONAL SERVICES FIRM

A Real-World Example

EXECUTIVE SUMMARY

In December 2016, ██████████ engaged CrowdStrike to investigate a ransomware infection at ██████████. CrowdStrike confirmed the malware within the environment was a variant of the SamSam ransomware, also referred to as Samas. CrowdStrike also identified additional activities associated with the tactics, techniques, and procedures of the xDedic Russian cybercrime group.

The main goal of the xDedic online forum is to facilitate the buying and selling of credentials for hacked servers and provide RDP access to cyber criminals. Once the buyer has purchased access to a compromised environment, they typically mount additional attacks on other networks or perform fraudulent Internet activities.

CrowdStrike identified RDP brute forcing activity on two hosts within the ██████████ Windows Active Directory domain. Additional evidence of the attacker performing fraudulent activities on Internet sites outside the ██████████ network was also discovered.

CrowdStrike did not identify evidence of data exfiltration. Additionally, the fraudulent activities identified were not associated with personal information belonging to ██████████ employees or clientele.



- **5,000,000 Encrypted Files**
- **Paid \$25,360 Ransom**
- **Backups Were Corrupted**
- **Down for Two Weeks**
- **39 Hours to Restore per TB**

SECURITY DEFINITIONS

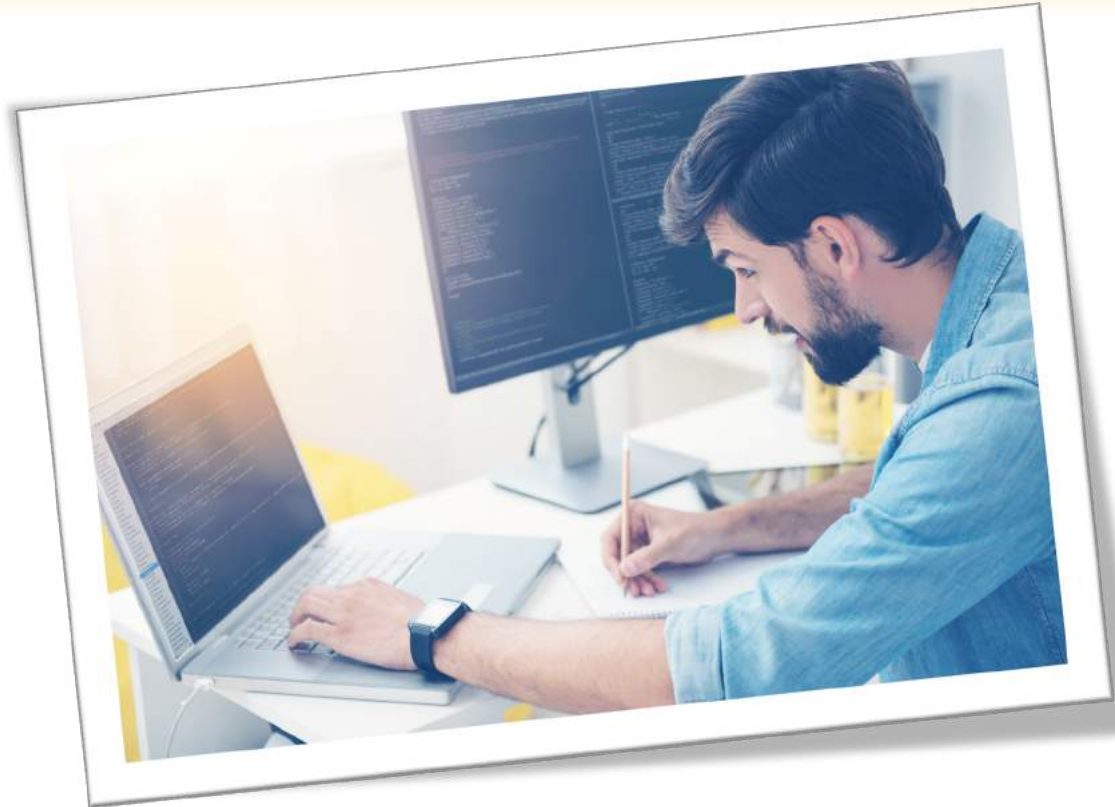


ENCRYPTION



Coding/scrambling the exchanged data to keep it secure from eavesdroppers. That means that while you are browsing a website, nobody can "listen" to your conversations, track your activities across multiple pages, or steal information.

DATA INTEGRITY



Data cannot be modified or corrupted during transfer, intentionally or otherwise, without being detected.

AUTHENTICATION

Proves that you communicate with the intended website. It protects against man-in-the-middle attacks and builds user trust, which translates into other business benefits.



TWO-FACTOR AUTHENTICATION



TWO-FACTOR AUTHENTICATION will help you to maintain your security online by requiring a second method of authentication like a code sent to your phone or from an authentication app to complete login.

COMMON TYPES OF CYBER ATTACKS

DENIAL OF SERVICE (DDoS) ATTACKS



A **denial-of-service** attack overwhelms a system's resources so that it cannot respond to service requests.

MAN-IN-THE MIDDLE (MitM) ATTACK



A **MitM** attack occurs when a hacker inserts itself between the communications of a client and a server.

PASSWORD ATTACK



BRUTE-FORCE password guessing means using a random approach by trying different passwords and hoping that one work Some logic can be applied by trying passwords related to the person's name, job title, hobbies or similar items.

DICTIONARY ATTACK a dictionary of common passwords is used to attempt to gain access to a user's computer and network.

EAVESDROPPING ATTACK



Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. Eavesdropping can be passive or active:

PASSIVE EAVESDROPPING — A hacker detects the information by listening to the message transmission in the network.

ACTIVE EAVESDROPPING — A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.

DRIVE-BY ATTACK



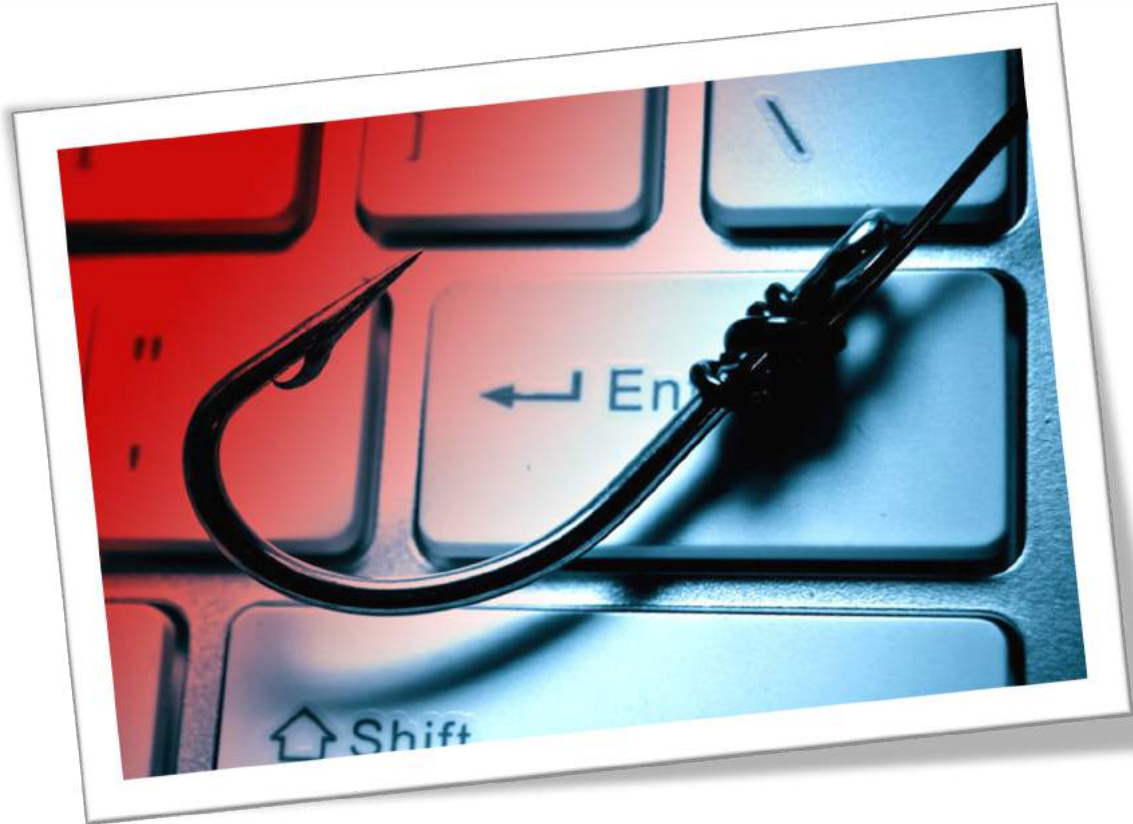
DRIVE-BY DOWNLOAD attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers.

MALWARE ATTACK



MALWARE is malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet.

SPEAR PHISHING ATTACK



SPEAR PHISHING is a very targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against.

PHISHING ATTACK



PHISHING ATTACK - is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

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.

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.



VARY PASSWORDS



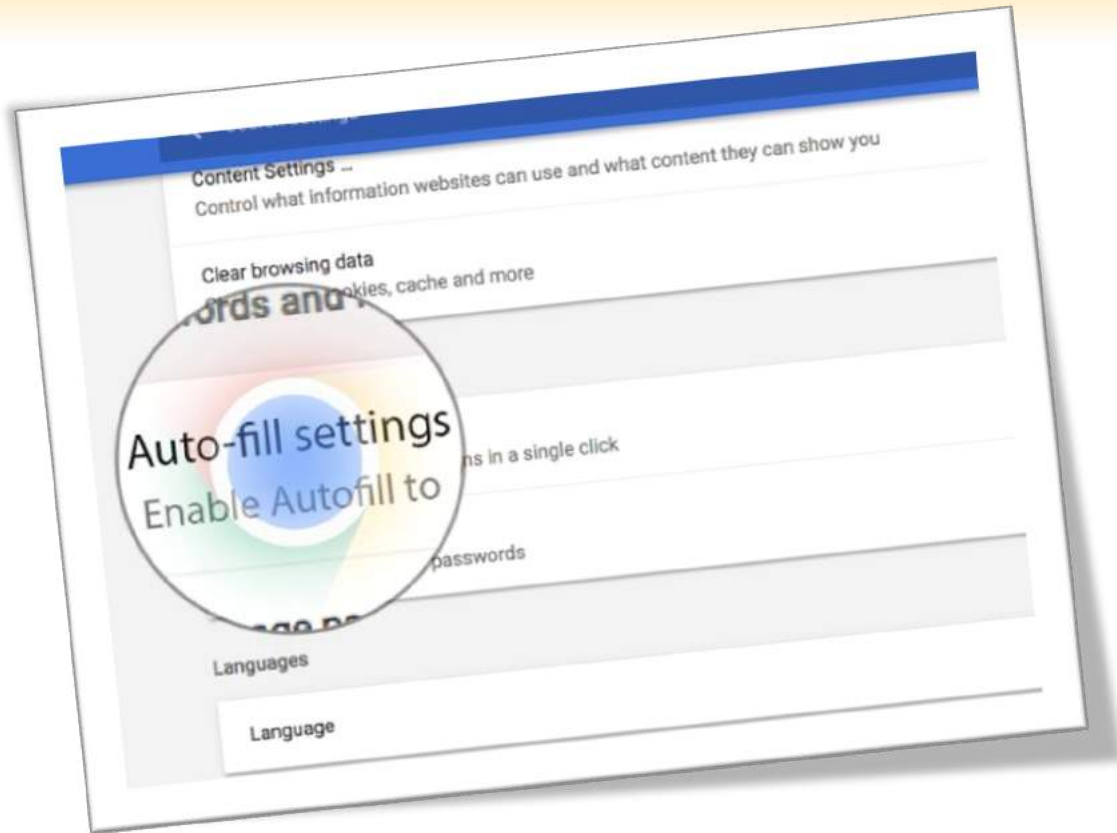
When you use the same password across many sites it makes it easy for criminals to hack all of your accounts. Use more complex and varied passwords for sites with personal information such as banking sites.

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*



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.

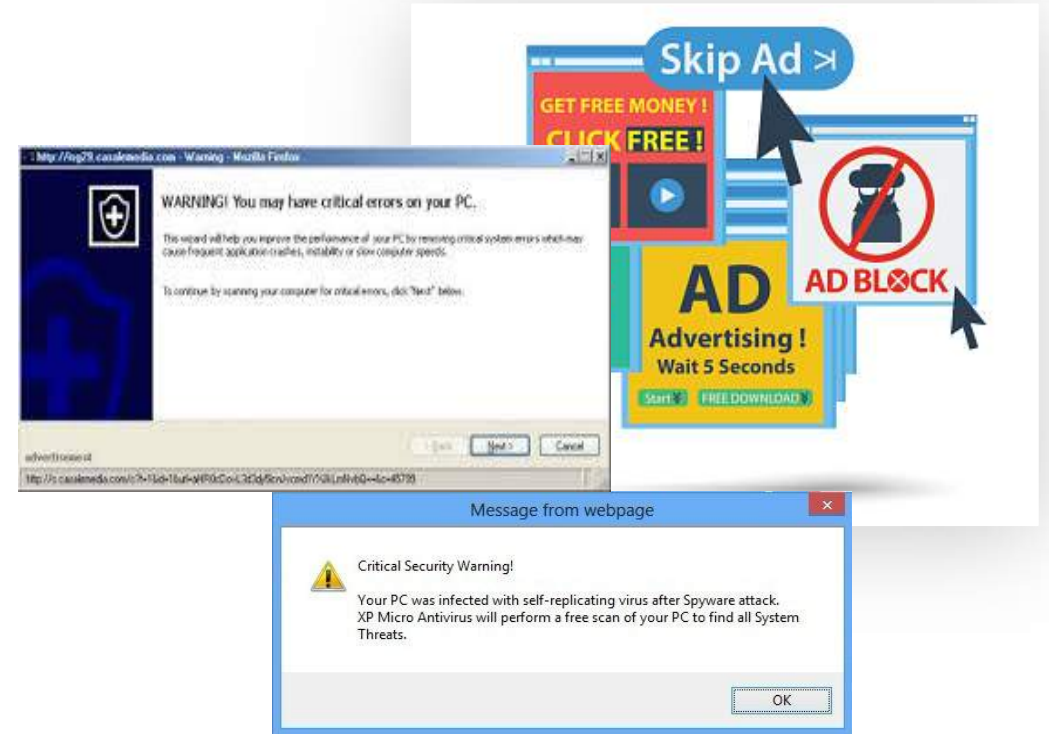
DON'T CLICK IT

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, antispymware, 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.



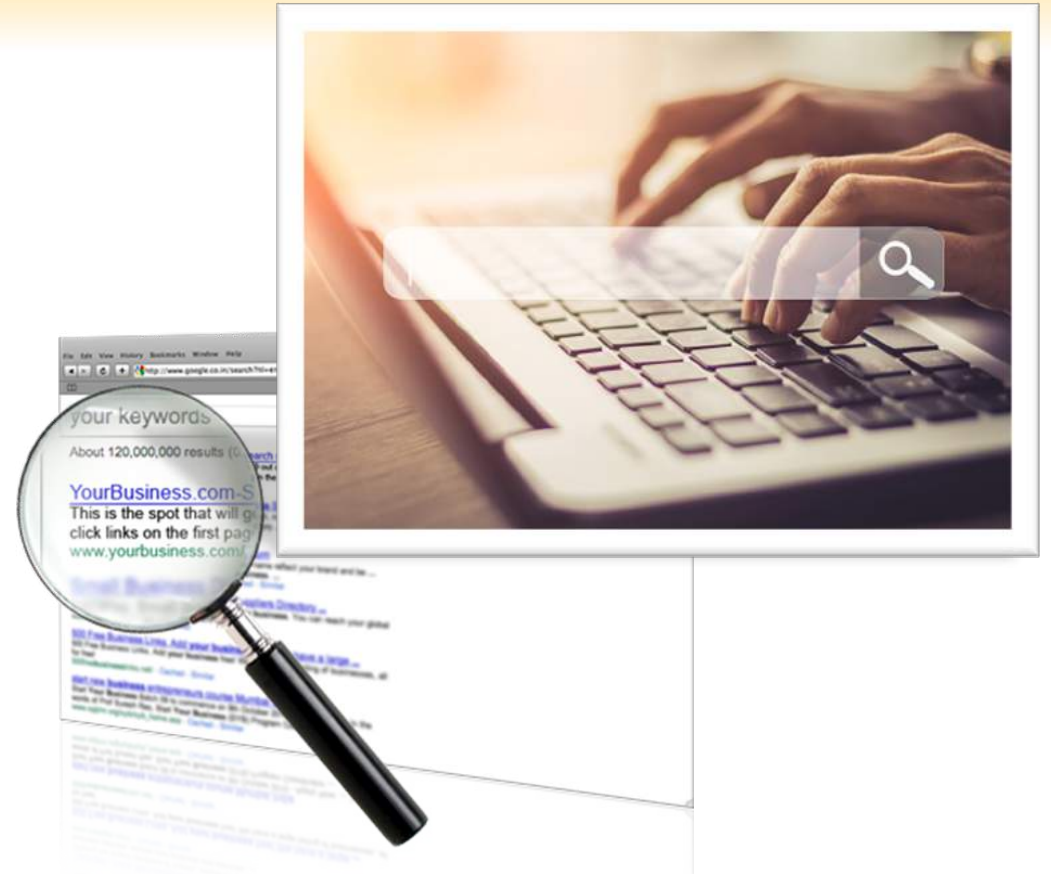
DON'T RUN IT

Beware of windows or pages that prompt you to click a link to run software. Malicious web sites 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 web site for scans and downloads.



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?

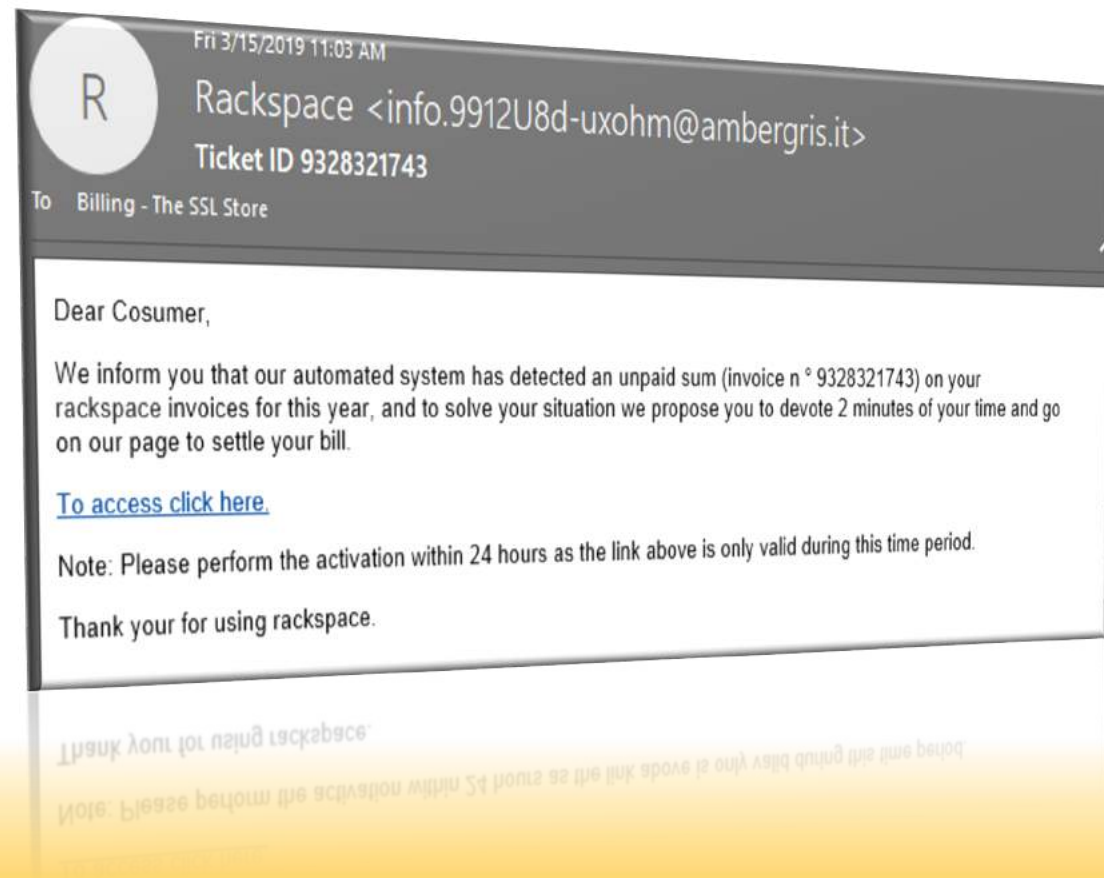
The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

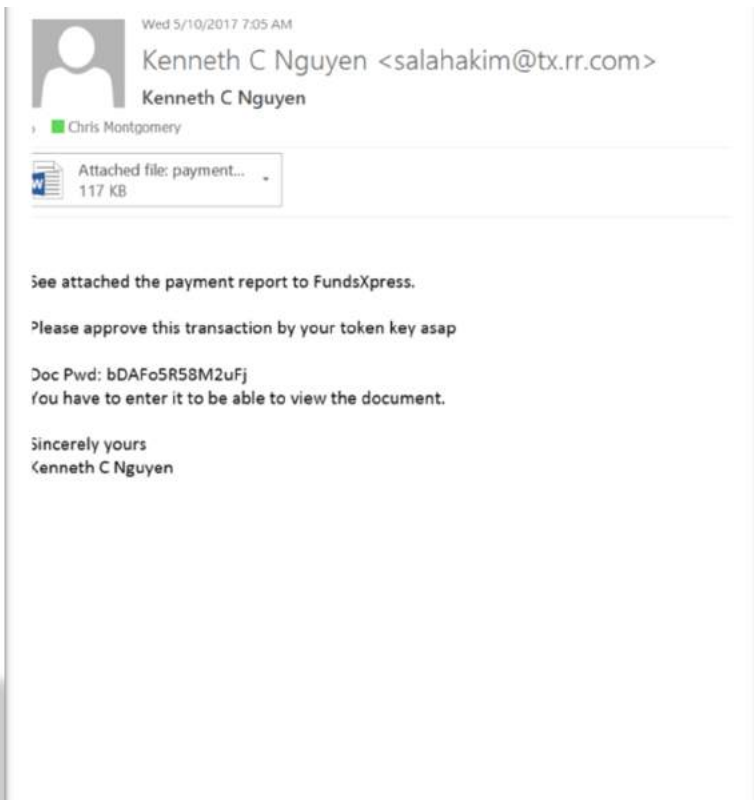
The variation we're discussing today is Social Engineering in the form of a phishing attack.



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





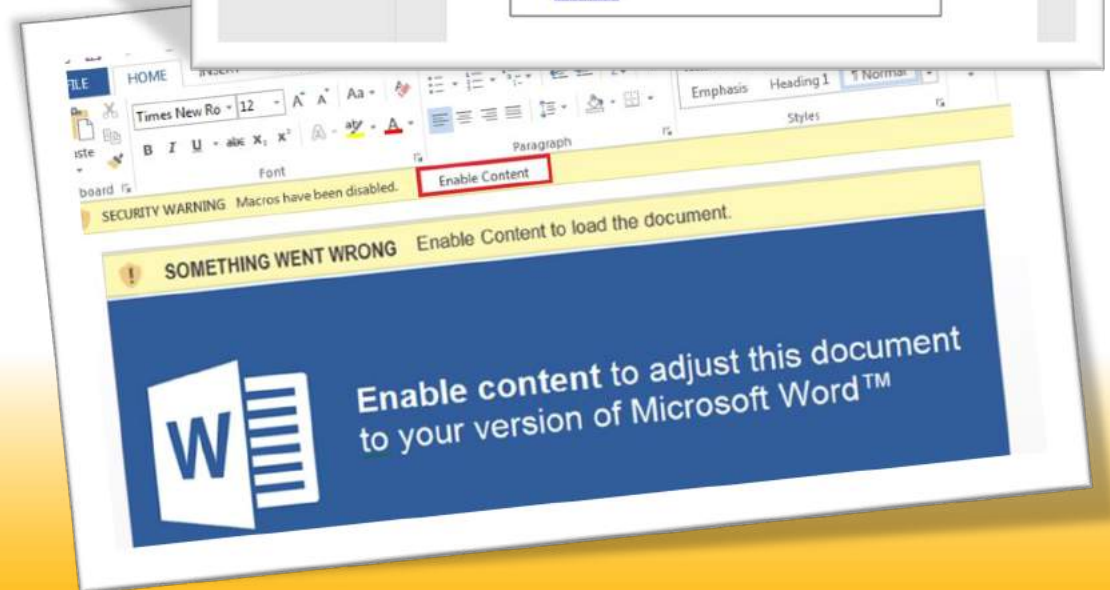
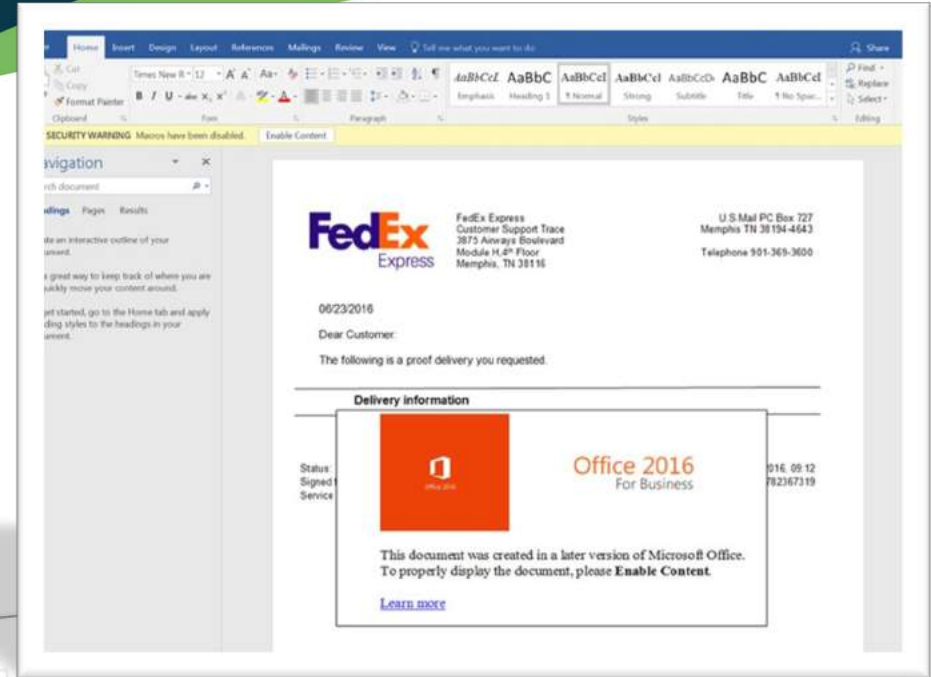
Example #1:

**Phishing Attack with
attachment in email Inbox**



Example #2:

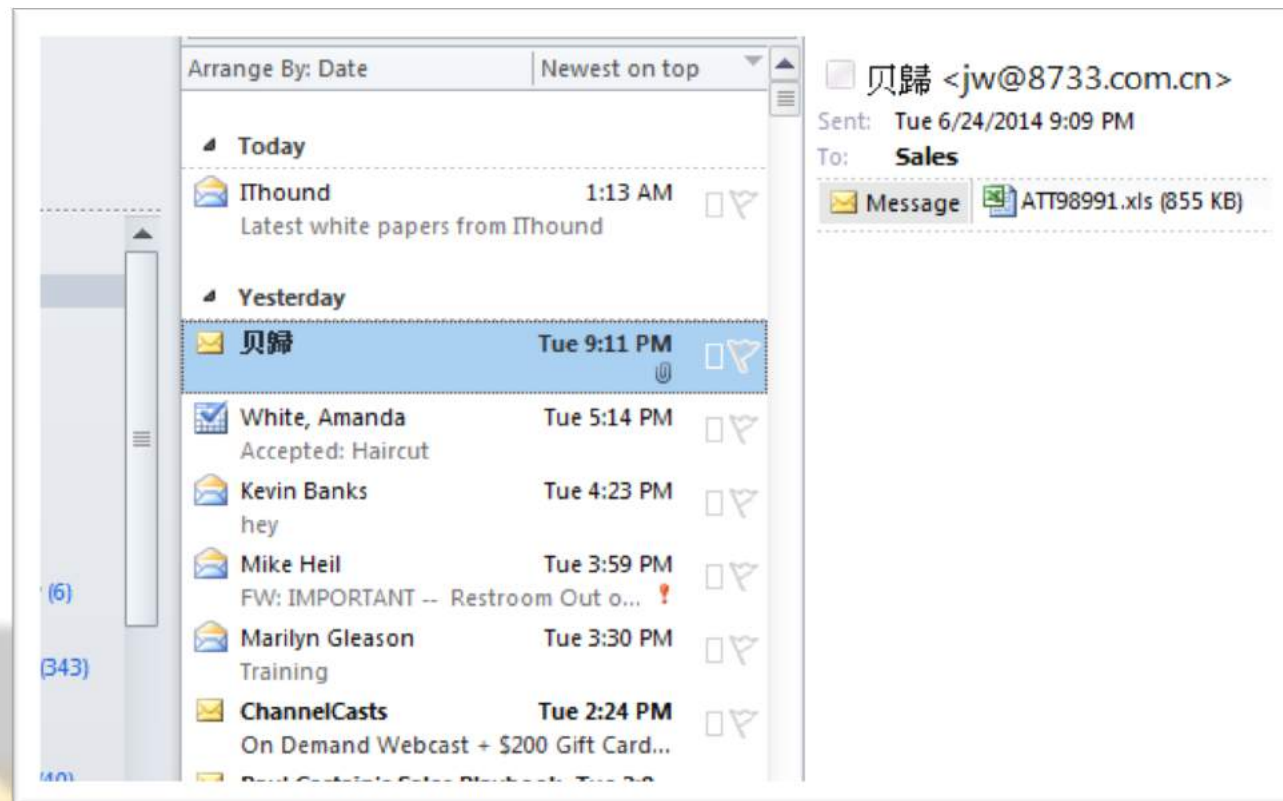
Phishing Attack from trusted source such as FedEx, Amazon, USPS or UPS





Example #3:

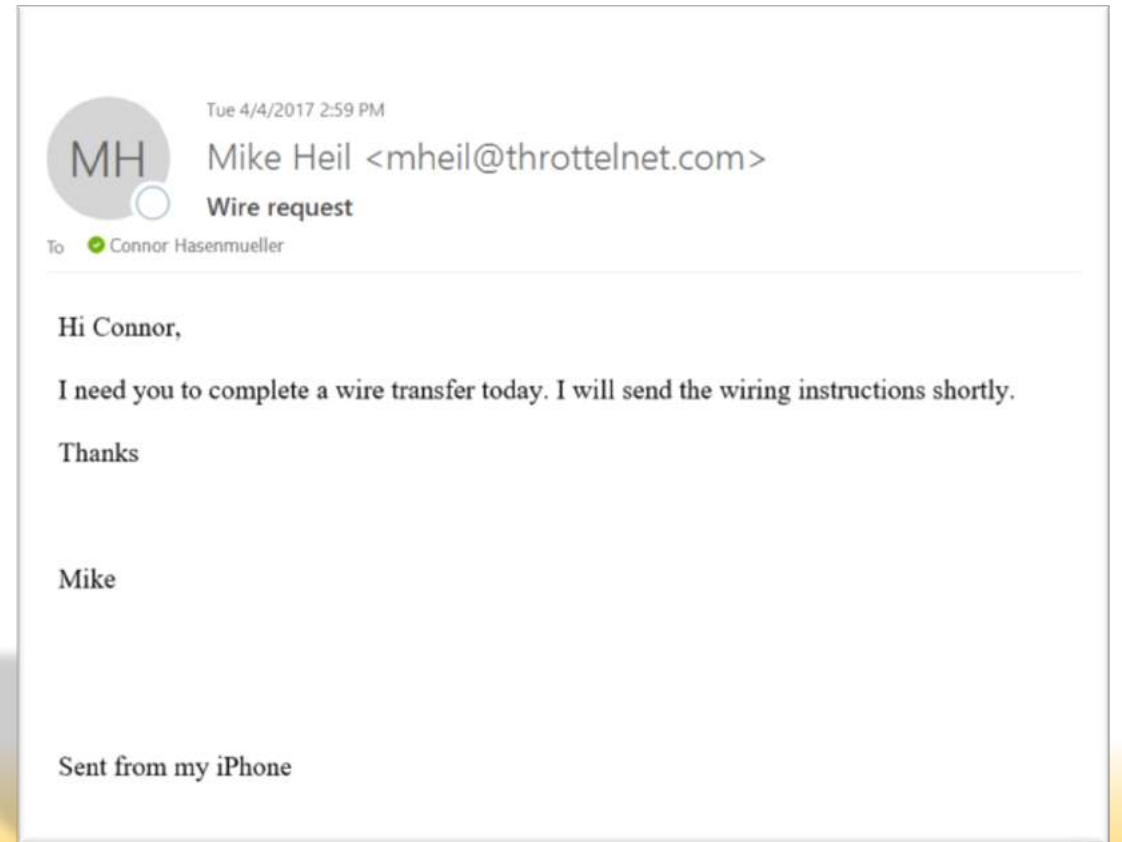
Phishing Attack from overseas with attachment in email Inbox





Example #4:

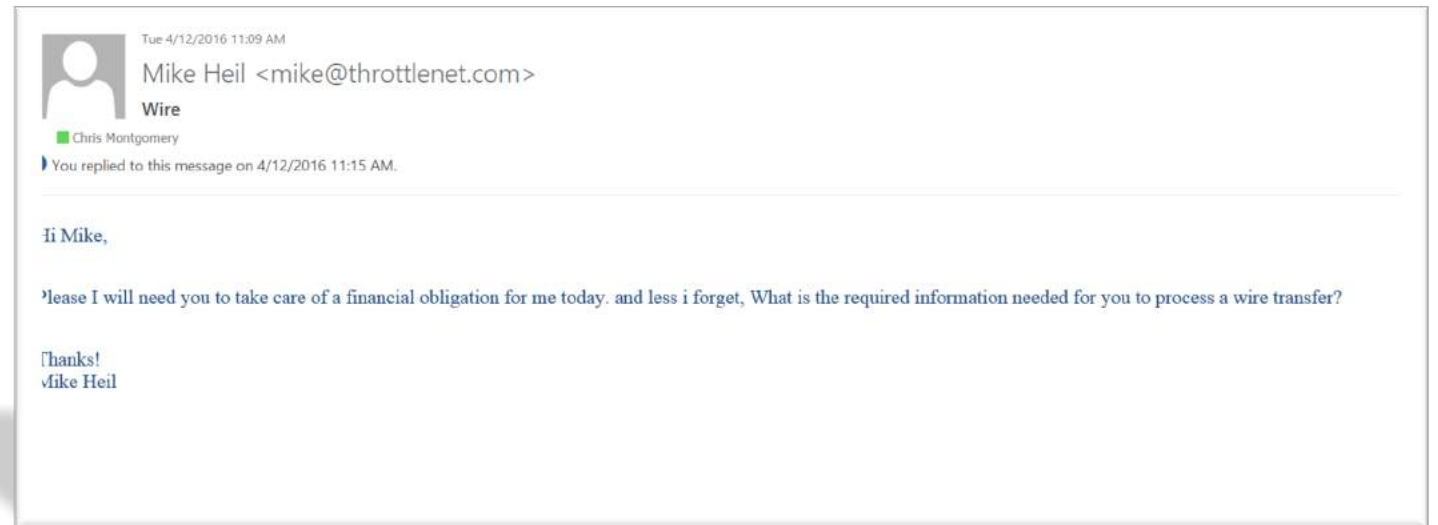
Phishing Attack with a wire transfer or gift card request





Example #4:

**Phishing Attack with
Attempt to gain information**





Example #4:

An actual interaction I recently had with a cyber criminal.

Bad Actor

From: George Rosenthal <managerexecutive1210@gmail.com>

Sent: Thursday, December 10, 2020 10:44 AM

To: Chris Montgomery <cmontgomery@throttlenet.com>

Subject:

Give me your cell phone number, I need you to complete a task for me.

Me

We've worked together for almost a decade and you don't have my cell number? You tell me all the time what a valued employee am I and yet, you don't know how to reach me.

You know what, I think I'm done here. Thanks for the memories and I'll see you next lifetime.

Bad Actor

I'm sorry about that, i change my phone which lead to loss of numbers

Me

I'm serious. 10 years I've been here and while I can appreciate the fact you lost your phone, I'm still done.

I don't care what you need since I don't work here anymore effective end of business today.

Bad Actor

I'm sorry about that, but can you leave that aside and help me with the task i ask of you?

Me

I've calmed down a bit and apologize. It's just so frustrating when you feel like someone really appreciates you and yet they don't have your number.

I guess I can help. What do you need?



STILL GOING.....

They don't give up and will take whatever you're willing to give.

Bad Actor

I need you to get a gift card, Can you arrange that now? So that I can tell you the product and denomination required.

Me

I'm pretty busy today as you can probably tell given my earlier frustration, but sure, I can try to work it in.

What do you need?

Bad Actor

That would be great thank you! Actually, what I need is \$1000 worth of Google play gift card \$200 in 5 places. You can get them from the store and send me the picture of the cards after you get them scratched.

Me

How am I supposed to pay for them? Out of my pocket? I don't have that kind of coin just laying around and given your history of reimbursing me, I'd rather not.

Bad Actor

I will make a refund when I'm through. If you don't have that much, how much can you afford?

Me

Given what you pay, not much. Maybe \$100.

Bad Actor

Ok, thanks. can you arrange that for me in the next 10 to 15 minutes

Me

You want me to get a gift card in the next 10-15 minutes? With the schedule you've got me on? How in the heck am I supposed to do that?

You should have said something yesterday when we spoke, but I guess since it wasn't the most pleasant discussion, it didn't make sense.

Speaking of which, I'm still angry about that. I mean, why in the world would you do that in the first place?

Sometimes I truly wonder why I still work here.....

Bad Actor

I'm sorry for the inconvenience, Take your time to get it and let me know when you have it with you



STILL GOING.....

But this time we didn't fall for it – and neither will you now that you know what to look for.

Me (the end)

Well aren't you sweet? Since you're so kind in letting me get it when I can, I'll repay the favor by asking you to kindly pound sand.

You're literally phishing a company that specializes in helping companies avoid phishing attacks. I plan on using our correspondence today as just one more example of how you work and what to look out for – so thank you for that.

In closing, I hope this back and forth prevented you from scamming someone else that doesn't know any better.

Merry Christmas.

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 login to an account from a link received in email, IM or social network

Never, ever login to an account after being directed there via a link received in an email, IM, or social networking message (i.e. Facebook).

If you do follow a link that instructs you to login afterwards, close the page, then open a new page and visit the site using a previously bookmarked or known good link.

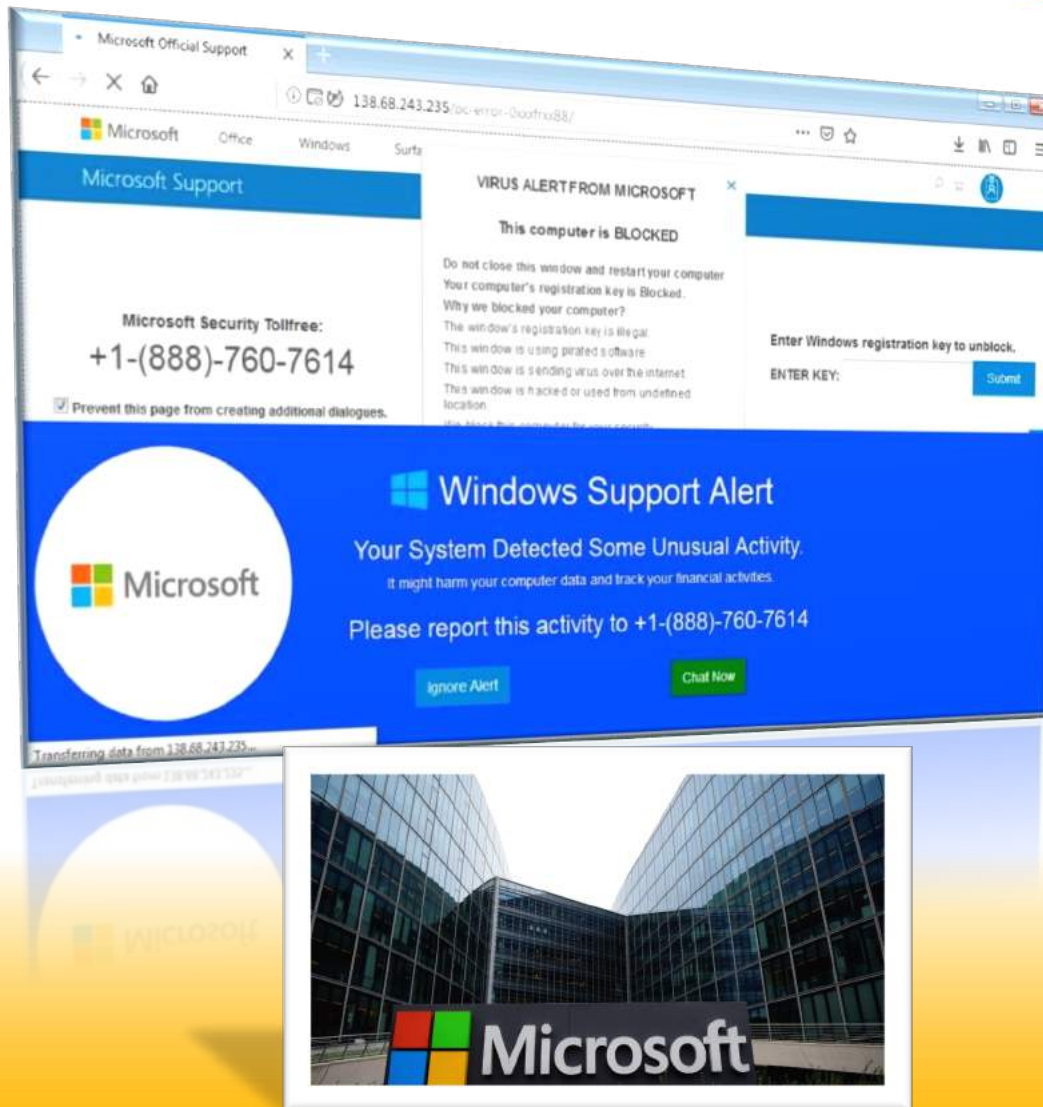


DON'T FALL FOR IT

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

HANG UP ON HIM!

Recommendation: Call the helpdesk if in doubt



HOW CAN WE

HELP?

866-829-5557

thomsonener

A man in a blue shirt is shown in profile, looking at a computer monitor in a server room. The room is filled with rows of computer monitors and equipment. The lighting is dim, with a blue tint. The text is overlaid on the left side of the image.

MANAGED SERVICES
BCDR SOLUTIONS
HOSTING SOLUTIONS
CYBER SECURITY SOLUTIONS

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



throttnet.com



throttlenet



throttlenet.com