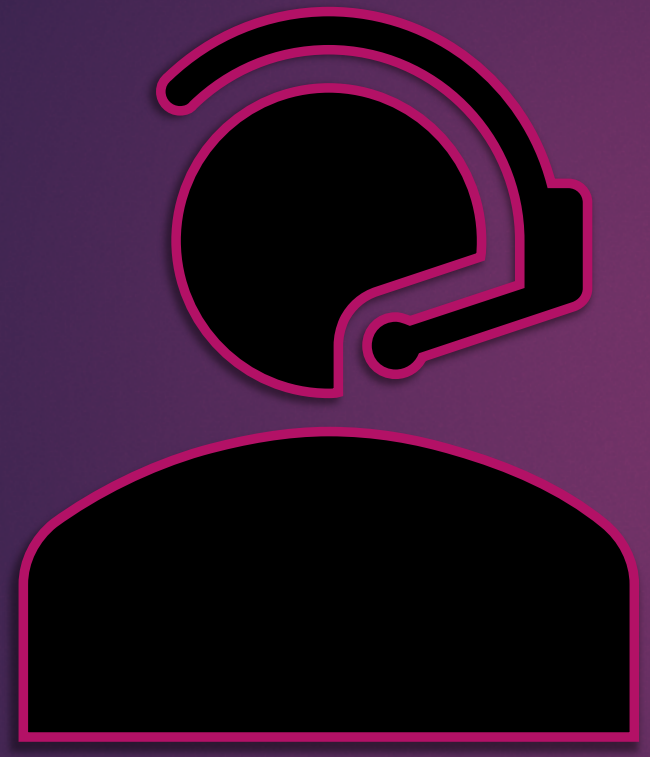
Cybersecurity

AN INTRODUCTION TO WORKPLACE ONLINE THREATS

Part 1



How It Affects You

YOU are the TARGET

- Office staff are the most targeted group as they have direct access to valuable information and systems.
- Email is the primary entry point of 94% of malware attacks.
- Cyber crimes increased by nearly 300% following the COVID-19 outbreak.
- Phishing accounts for 80% of reported security incidents.
- Human error is the primary cause of cybersecurity breaches, accounting for 95% of all data breaches.

Cybersecurity is **EVERYONE'S** responsibility

Part 2

Types of Cyber Attacks

Business Email Compromise

- Also known as a "Man-in-the-email" attack
- In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, like in these examples:
- A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his down payment.

Business Email Compromise - Protect Yourself

- Don't click on ANYTHING unsolicited asking you to update or verify account information. Look up the company's phone number on your own.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust. (Hover your mouse over the email address)
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.

Phishing attack

- Here, we see an example of a classic phishing attack. Phishing attacks are emails sent from attackers pretending to be someone else. For example, they might impersonate your bank and send an email to you that appears to be from your bank. When you click the link they send, and put in your username and password, it sends your credentials to the criminal.

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

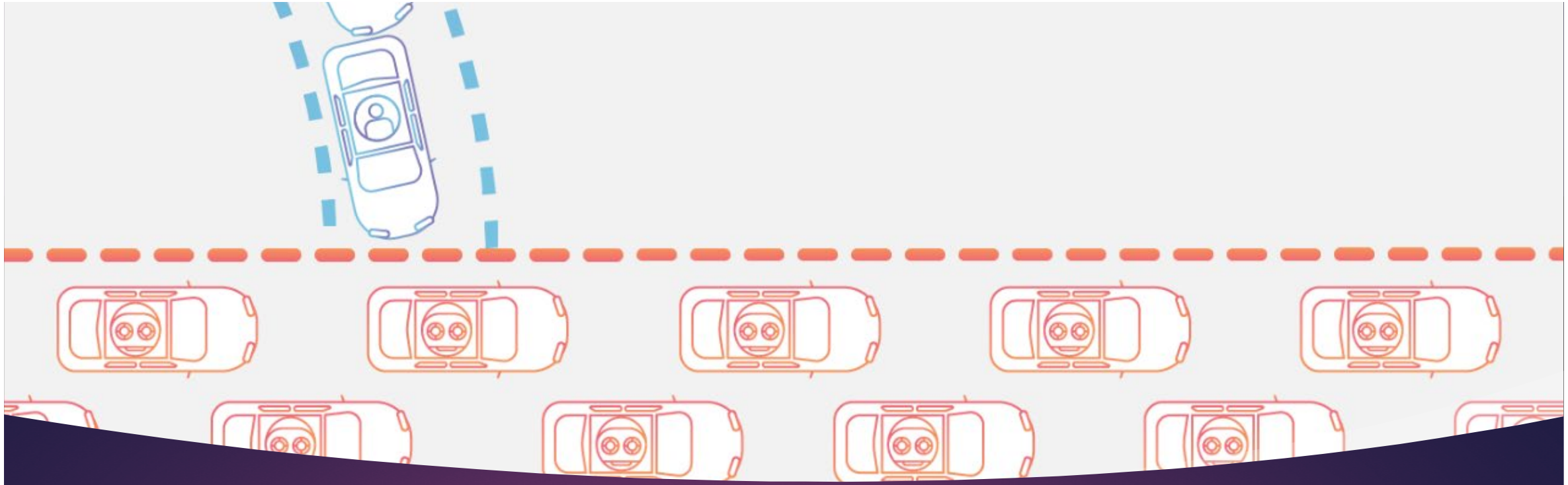
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Ransomware

- Ransomware is a computer virus that attacks the file system of a computer. The virus will work its way through your computer and locks up every file and program on your PC. This leaves your Computer unusable. The virus can spread its way through your network and lock up every computer on your system. The attacker has the password to unlock every file in your network, and will usually demand a ransom to unlock it.



Denial of Service attack

- Denial of service attacks (DOS attacks) occur when an attacker overloads your network with data packets. This renders the attacked network unusable. This can lead to huge financial losses for the affected organization, as any services they offer will be completely unusable. Aside from financial loss, there is no other long-term, negative effect resulting from this attack. A DOS attack that comes from multiple computers around the world is referred to as a Distributed Denial of Service attack (DDOS attack). These are far more effective and can prove to be much more difficult to stop.

Part 3

Tips to keep you safe

Be careful what you click

- Avoid going to unknown websites
- Avoid downloading software from untrusted sources
- If the link is unexpected, DO NOT CLICK IT
- This is relevant for email, websites and text messages

Keep software up to date

- Installing updates in a timely manner prevents bad people from getting into your system with known vulnerabilities.

Strong Passwords

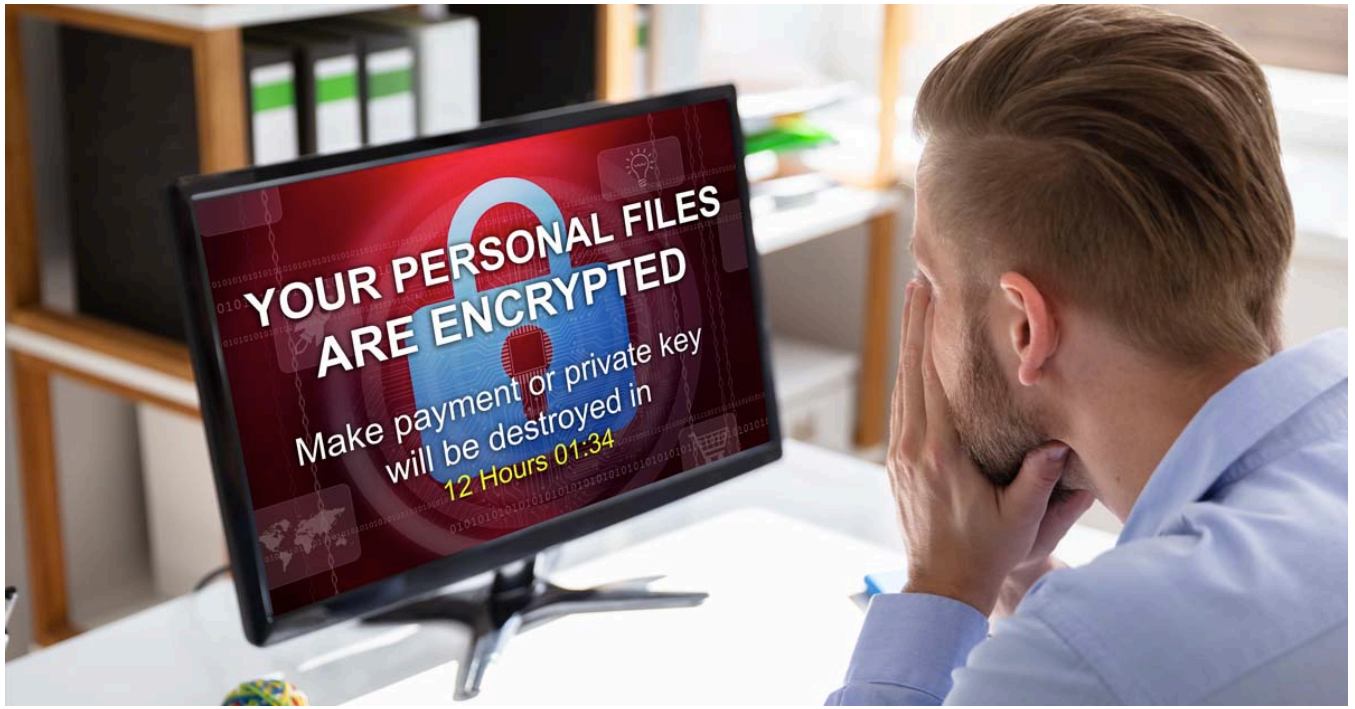
- Use long and strong passwords.
  - Password should not be related to you in any way
  - 20 characters or more are recommended
  - Use upper case, lower case, numbers and special characters
  - Do not use the same passwords for multiple accounts
  - Try to avoid using dictionary words for passwords
- Use trusted password managers
- Do not give your password out
- Do not leave your password written down at your desk

Unplug

- **If attacked, or if you think you might be currently experiencing an attack, simply pull the Ethernet cable from the computer, but do NOT turn off the computer.**

Backup

- **ALWAYS have offline backups. These backups should not be associated with your network in ANY way. If your backups are online, there is a good chance they have already compromised those as well. Once your backups are compromised, there may be no coming back. So always have an OFFLINE BACKUP!!!**



Resources

- StopRansomware.gov