RETIRED DETECTIVE GEORGE CHAVEZ
CYBER SECURITY TRENDS 2024
MADISON CREDIT UNION

AGENDA

- Introduction
- AI and the impact on Cybersecurity
- Scams: Student Loan Scams/ Phone Scams/ Text Scams/ Crypto Scams/ Cash App. Scams/ Online Purchase Scams/ Employment Scams
- How to make your Cyber journey safer: What to be aware of and things to look for.
- Best ways to prevent others from accessing your information.

Detective Chavez received his certification from the EC Council as an ethical hacker in 2017 conducted in Washington DC.

In retirement, Detective Chavez is now a chaplain serving the community and is asked to provide training in trauma, service and expertise in gangs, narcotics, social media and general cyber security.

TERMINOLOGY THAT WE SHOULD KNOW

- **Phishing:** A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. (National Crime Security Counsel)

- **Deep Fake:** Deepfake AI is a type of artificial intelligence used to create convincing images, audio and video hoaxes. The term describes both the technology and the resulting bogus content and is a portmanteau of deep learning and fake. (Tech Target)

- **Passkeys:** These will replace the passwords we keep on our computer to allow a safer place to store passwords on a device that can be plugged into your computer.

TERMINOLOGY THAT WE SHOULD KNOW

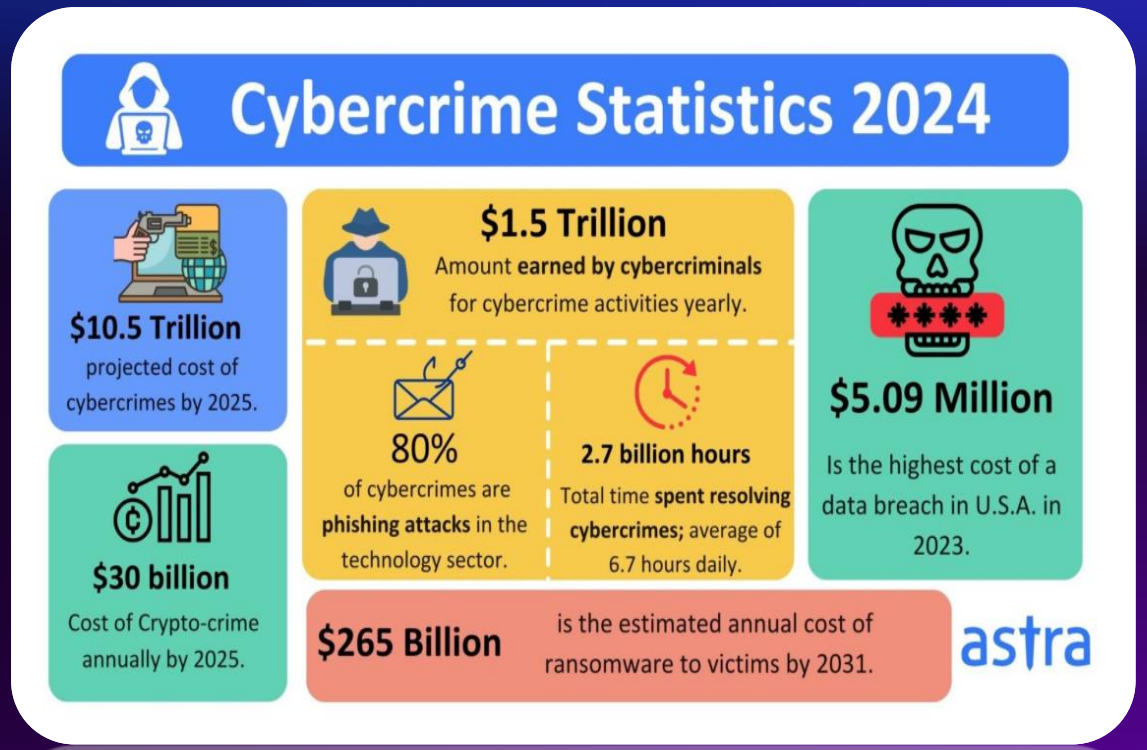
- **Malware:** Short for malicious software, refers to any intrusive software developed by cybercriminals(often called hackers) to steal data and damage or destroy computers and computer systems. (Sysco Security)

- **Ransomware:** type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid. More modern ransomware families, collectively categorized as cryptoransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decryption key. (Trend Micro)

WHY IS CYBERSECURITY IMPORTANT?

Statistics

- According to the FBI Internet Crime Records, over 422 million individuals were impacted by cybercrime in 2022.
- Nearly 33 billion accounts will be breached with the cost of these breaches predicted to be close to 8 trillion dollars.
- A cyberattack occurs roughly once every 39 seconds.
- Cybercrime rates have increased by 300-600% since the beginning of the covid-19 Pandemic.

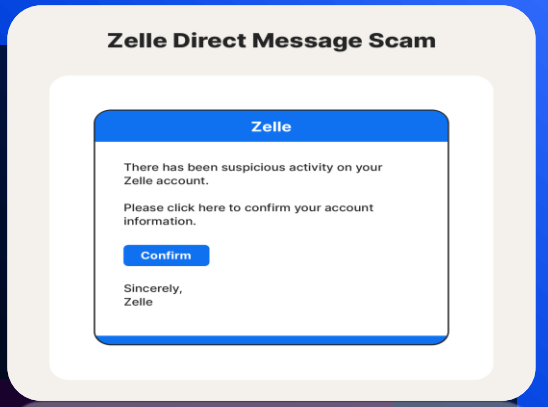


References: Astra Security Blog

CAUSES

- Remote working led to 47% of cyberattack victims falling for various phishing attacks. Remote work has also resulted in an increased average of data breaches.
- An increase in daily phishing and malware related to Covid-19. Google actually reported they blocked at least 18 million of these emails.
- An increased use of IOT devices and connections.
- The most common cause of cybersecurity breaches are caused by human error. Some report 9 out of 10 cybersecurity breaches are caused by human error.
- Advances in Artificial Intelligence has greatly impacted the sophisticated way hackers and cybercriminals have been able to take cybercrimes to higher levels impacting more victims.

Most common cyber scams trends to look for in 2024



Peer to Peer Payments

- If we are being honest, we continue to move towards ways of making life convenient. This includes buying and purchasing items as well as buying and purchasing services. It is important to be aware of the security of the types of applications that are utilized by the those paying for services as well as those providing the services.
- These applications, such as Venmo, Zelle or Paypal, that are directly connected to your banking institution, means you have now created potential opportunities for additional exposure of your information. These types of accounts are also connected to social media accounts which again provide another level of vulnerability of information.
- The device you are using is also a consideration. Some experts share, you should have one device for your banking, credit card and any other financial transactions, and another, separate device, for social media and online searching.

AI-ENHANCED SCAMS

Technology has now provided a more sophisticated way of producing emails, text messages, and calls, to convince the victim they are valid. They are in tune with events and things happening throughout the world which again makes them more believable.

AI-ENHANCED SCAMS

Some known Scams we hear about today:

1. **Student Loan Forgiveness Scams**: Many know of the government's program and the many young people who are emotionally tied to this program. Criminals prey on them in attempts of stealing their Social Security Number or bank account information. They will use pressure tactics, like many scams do, and attempt to convince you the response needs to happen in a certain amount of time, usually immediately.
    - *It's important to slow down and read any email or message carefully. And to know the rules various organizations have when it comes to these notices, especially, when it comes to government agencies. They will list how they will contact you and the steps they take.

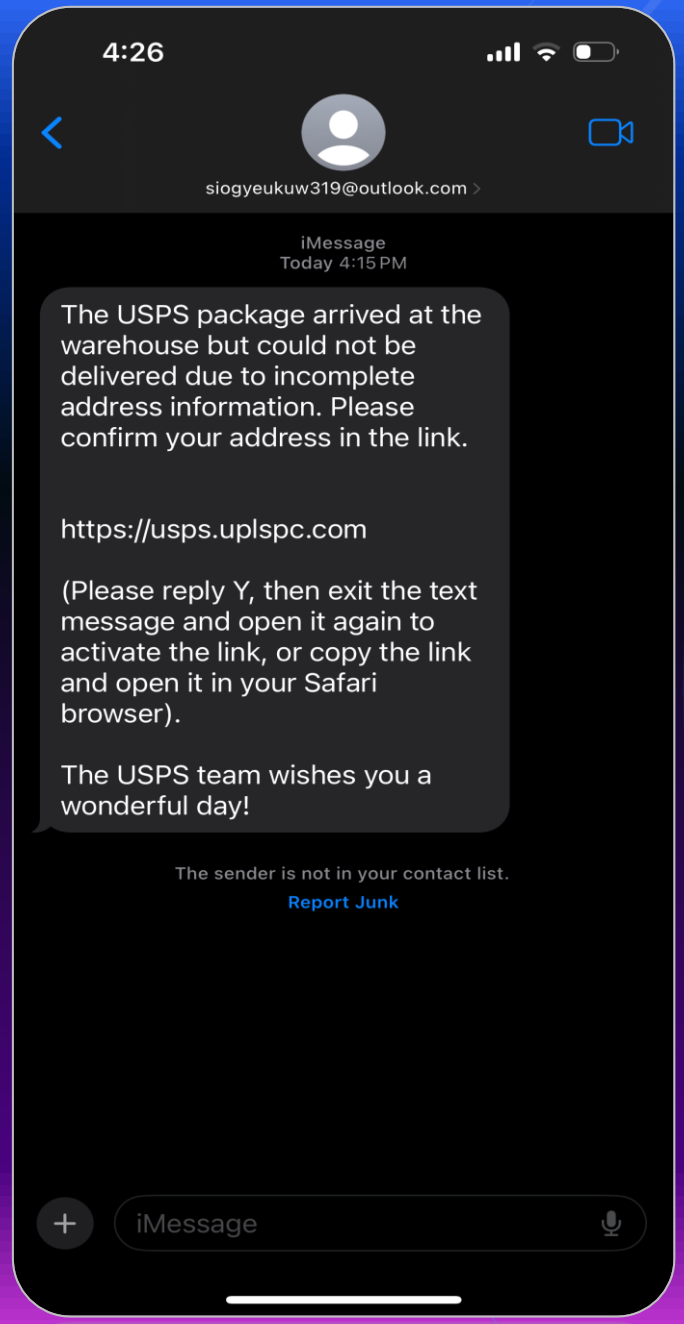
2. **Phone Scams:** We have all experienced those annoying calls with recorded messages, and callers sharing information on things you have not even inquired about. How many of us have received calls that we are going to be arrested, or will suffer severe penalty if we don't pay a penalty, or the policeman's fund recording?

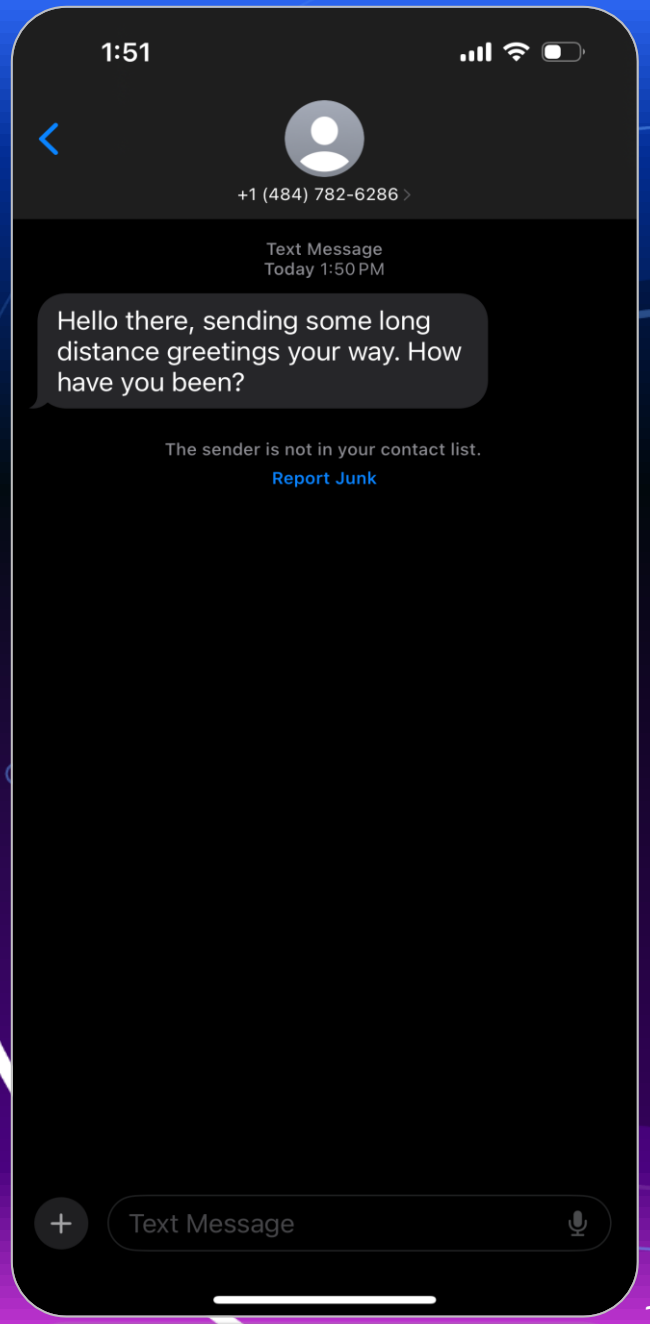
3. **Impersonators or Apps:** People attempting to be someone they are not, IRS, delivery services, relatives. ***Be careful what you download.*** Cybercriminals are always looking for vulnerabilities. An up-and-comer is QR codes, which can be used to direct you to what may appear to be an authentic site, but instead is a site built by a criminal to collect your sensitive data and information.

Experian, 2024

EXAMPLES

What are some things you notice?





AI-ENHANCED SCAMS

As is often said, “If it’s to good to be true, then it probably is!”

4. **Crypto Scam:** Unless you are very familiar with cryptocurrencies, it is best to stay away from them. AI is utilized in cryptocurrencies to get you to buy into an investment or get you to disclose any cryptocurrencies you have where you will then be exposed to an “OTP bot attack”.
    - An “OTB bot attack”, similar to ransomware, locks you out of your account while the cybercriminals empty it. It’s not uncommon for them to leave malware which will allow them to gain access after the initial crime has happened. It leaves what I would call an open access point to return to do more crime.

AI-ENHANCED SCAMS

5. **Online Purchase Scams:** The FTC reported that 44% of social media scams from January to June 2023 were related to online shopping. At times, the scammer will play the role of the seller, this is seen quite often on Facebook Marketplace. I, myself almost fell for one (*Treadmill Story*). Many time's people send money before actually receiving the product, and then learn there was no product, and their money and post are gone.

6. **Employment Scams:** As we have shared, cybercriminals target the vulnerable. This scam is no different, it focuses on people who have been out of work or have been struggling for some time. Potential employers (cybercriminals) act as if conducting an interview or ask you to fill out an application and get access to your information.

EXPERIAN, 2024

WHY SO MUCH FOCUS ON SCAMS?

When it comes to cybercrime, our individual vulnerabilities can have a big impact on our personal finances. Whether you are doing your personal business or your work business, it’s important to remember most of the vulnerabilities are due to human error.

So, what are some steps that we can do to help make us less vulnerable to cybercrime?

BEST WAYS TO PREVENT OTHERS FROM ACCESSING YOUR INFORMATION.

- **Do not share your personal information with anyone**, especially any institution you do not know or have not interacted with, this could include charities, banks, or any financial institution that you cannot verify.
- **Passwords should be a minimum of 20 characters.** Remember, cybercriminals utilize many programs to attempt to gain access to your password. They do their homework, and can tell your interests as well as potential birthdates, locations, phone numbers, etc.
  - Instead, think about sentences you can remember, do not post or complete information on social media such as surveys about your personal life.
- **Never click on links in emails or text messages before you have verified them**. Authenticate the message is actually from who you believe it to be. Ensure that email addresses, phone numbers, and sites actually match the addresses that have been given by the individual in the email. Most offer two-factor authentication, use this!
- **Do your homework.** Most current scams are often shared in the news. Be sure to create with family, even extended family, a password you all know, that if anyone needs help, grandparent scam, they will be able to share the password.