Cybersecurity

Tariq Azmi

Overview

- Introduction
- Statistics
- Finance & Banking
- Email Hijacking
- Social Engineering
- Ransomware –
- Myths about Cybersecurity
- Cyber Hygiene

Tariq Azmi

- A technology operations entrepreneur who works with the compliance industry to ensure regulatory compliance, data integrity, and business continuity. Founding partner of Ember Technology.
- Over course of 15 years worked in all aspects of the IT, from support desk, project management, data analysis, etc. Worked for the Kansas Bureau of investigation where the trajectory changed and gained much knowledge and experience in Cyber Security, compliance, and Digital Forensics.
- Tariq is RP with the CMMC – AB, have been working in the Defense Industrial Base (DIB) providing added value in cyber security & compliance to companies working with DoD

Statistics

Cybercrime is putting every organization at risk for financial damage, regulatory fines, tainted customer relationships, reputational loss and infrastructure harm

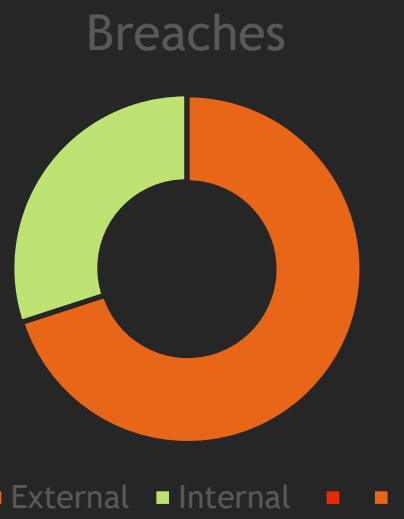
Statistics -

Remember 70/30

70% of the data breaches are caused by external cybercriminals

Many external breaches are prompted by money and access to data

30% of the breaches involve internal cybercriminals



Statistics

Having an Incident Response plan in place will better equip a company in their recovery.

More than 77% of organizations don't have a Security Incident Response plan in place

Companies who respond to an attack within 30 days **save an average of $1M**

Of the organizations that do have a plan in place, more than half don't test their plans regularly.

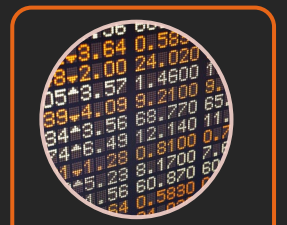
Statistics

On Average most companies take more than 6 months to detect a data breach

Financial Industry takes an average of 98 days to detect a breach → The retail industry takes up to 197 days → The education industry takes up 217 days → The healthcare industry takes up to 255 days → The entertainment industry takes up to 287 days

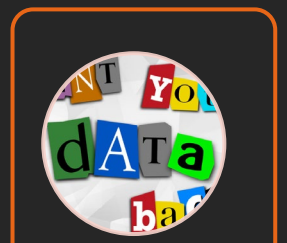
During that time, bad actors can:

Conduct Surveillance



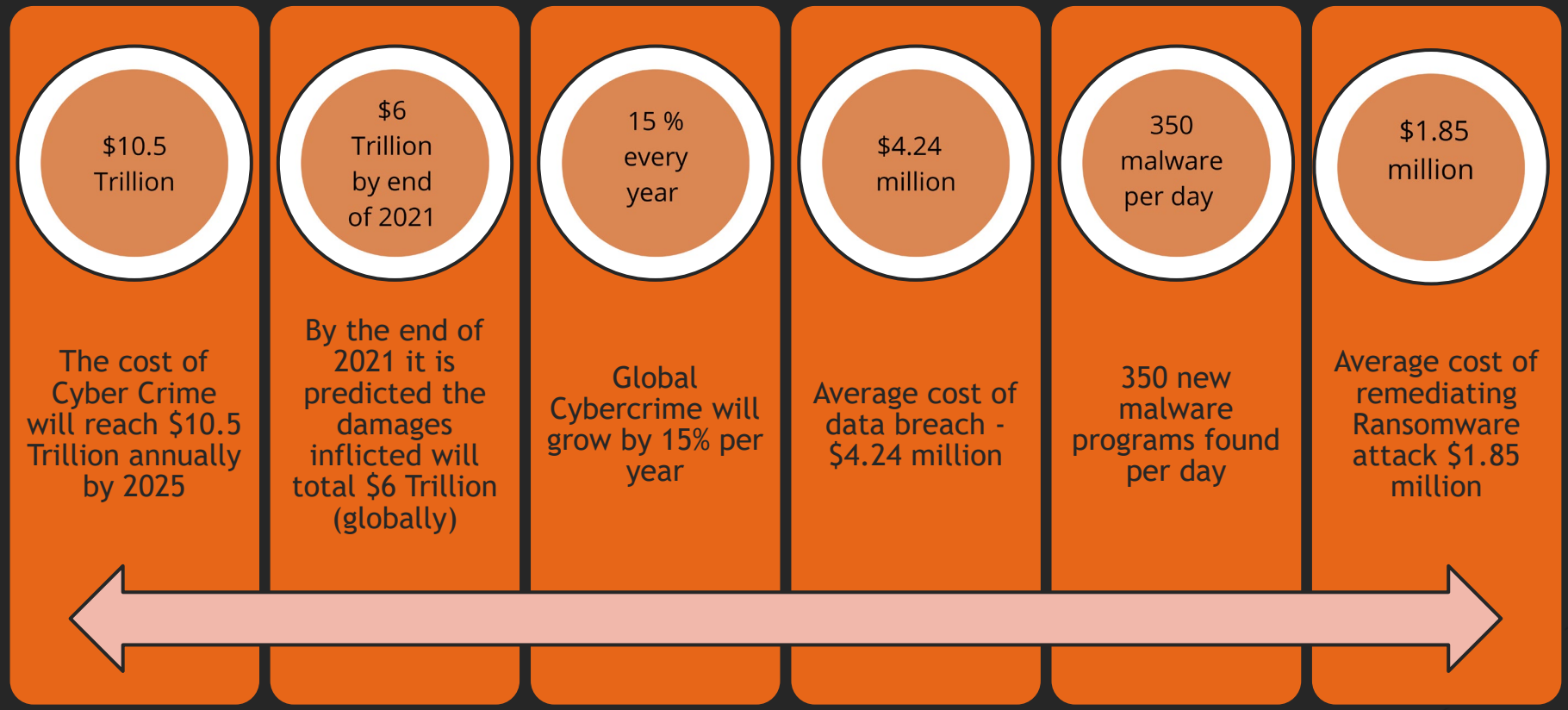
Steal Data

Spy on Companies



Ask for Ransom

Statistics


$10.5 Trillion
The cost of Cyber Crime will reach $10.5 Trillion annually by 2025
$6 Trillion by end of 2021
By the end of 2021 it is predicted the damages inflicted will total $6 Trillion (globally)
15 % every year
Global Cybercrime will grow by 15% per year
$4.24 million
Average cost of data breach - $4.24 million
350 malware per day
350 new malware programs found per day
$1.85 million
Average cost of remediating Ransomware attack $1.85 million

Financial Industry

The Ongoing Battle Between Security and Convenience

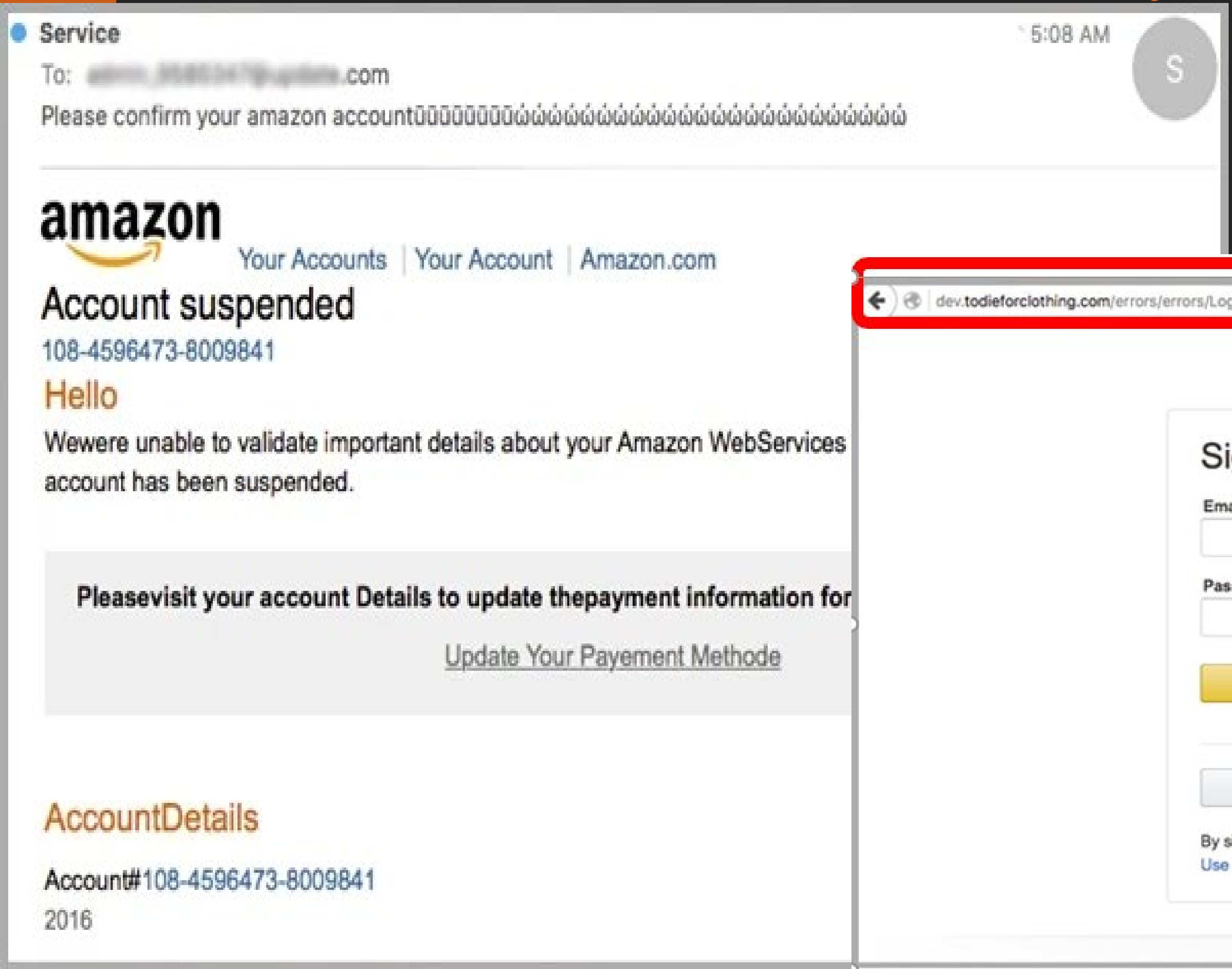
- Ease Satisfies End Users Need for a Positive Experience —
- Challenges
  - During COVID fintech app usage is up 72% since the start of the pandemic. That means more data to manage, more opportunities for man-in-the-middle attacks, and more storage locations that must be protected.
  - During COVID many user are more concerned right now about their health than their data.
  - Many of cyber criminals would rather break into bank accounts than homes, and a lot of fintech data looks ripe for the taking. Many apps were built with business needs in mind first, security concerns second.

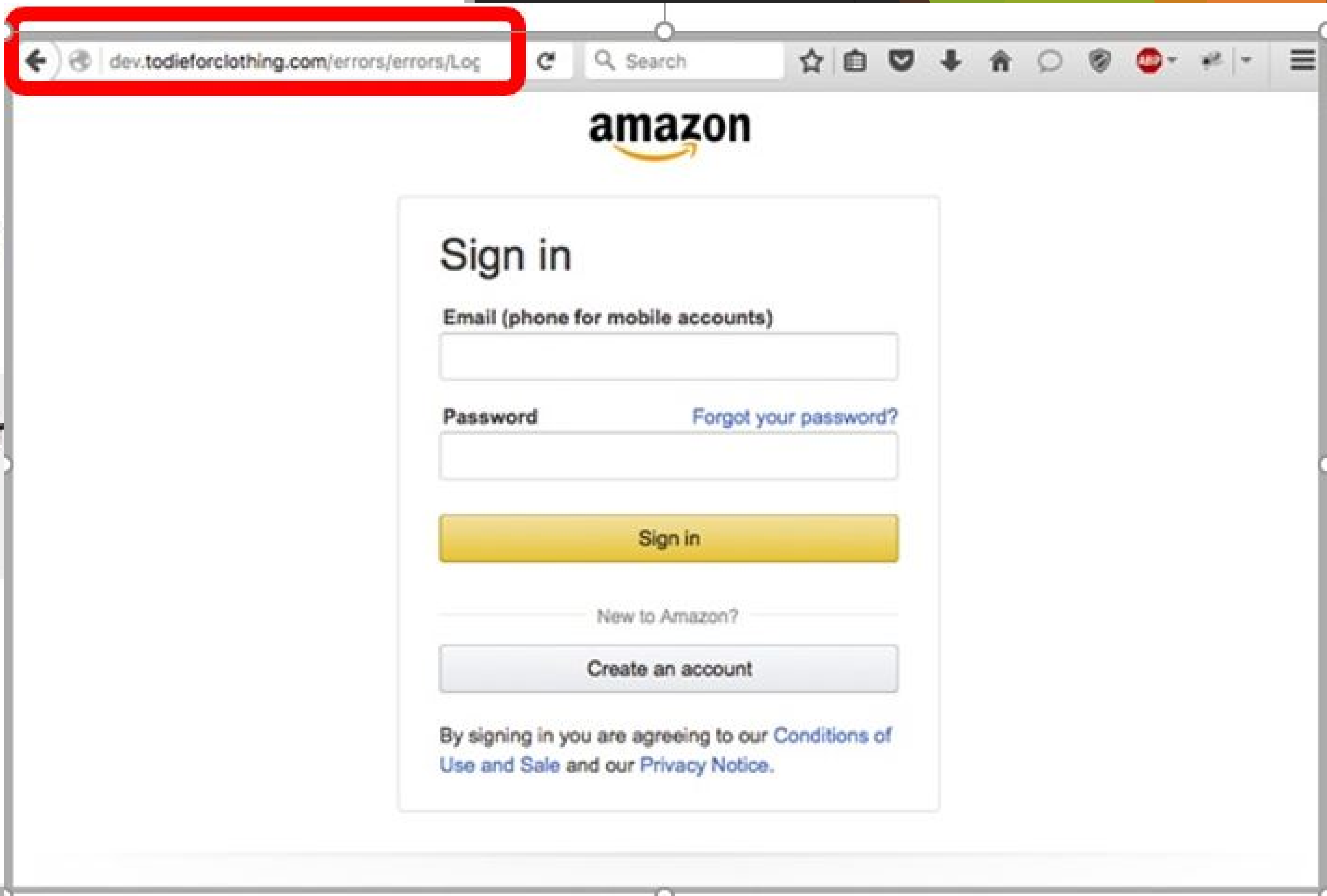
Financial Industry

Easy can be risky, if enough thought hasn't gone into the user experience.

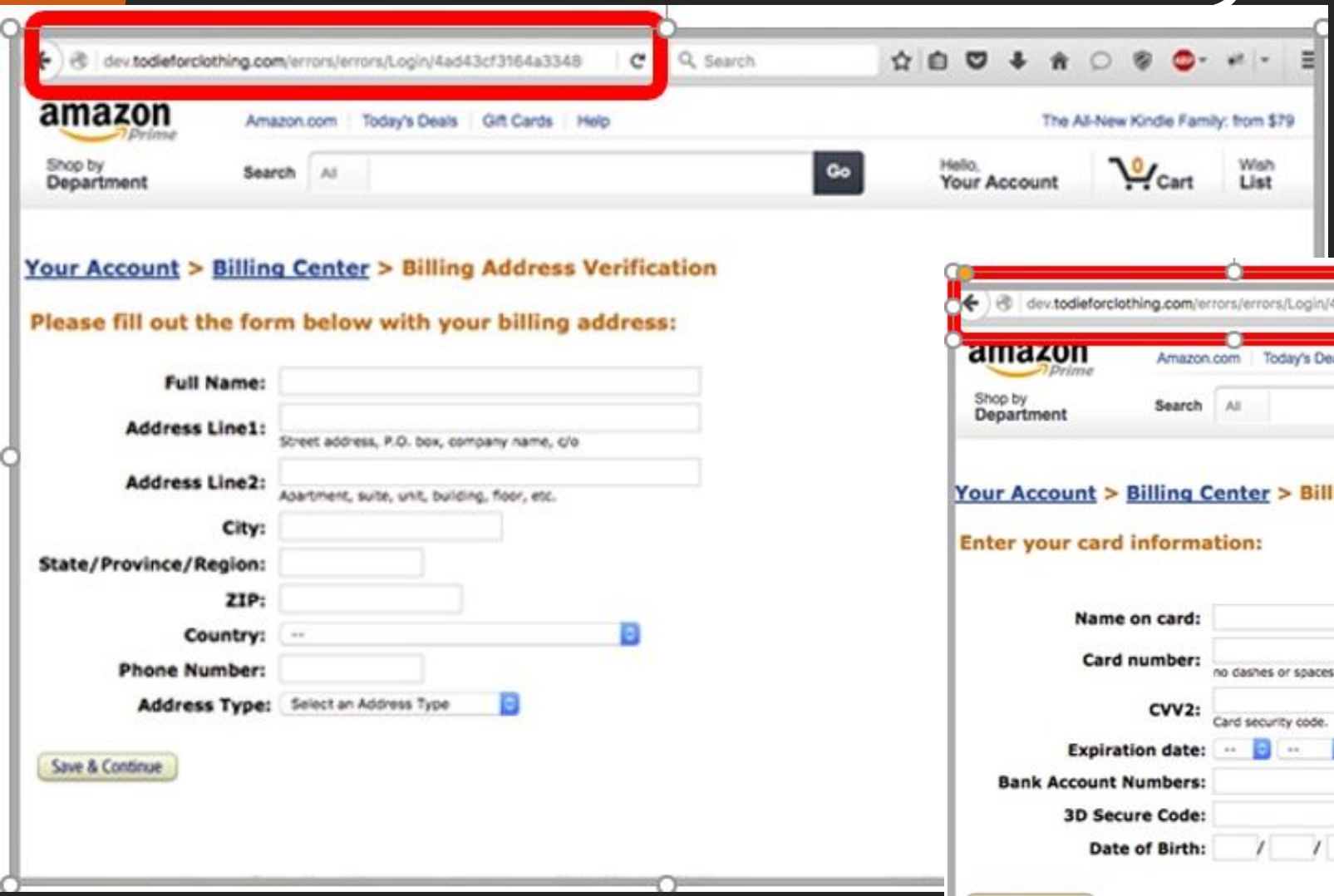
- Solutions:
  - Multi Factor Authentication
  - **Long Password** at least 12-18 characters (MyFavshowin2021Squ1dGames!)
  - Security Settings
    - Financial APP
    - Robinhood
    - Paypal
    - Zelle
    - Venmo
  - Shopping: Do not save you financial Information
  - Consider your Payment options
  - Keep tabs on your Bank and Credit Card statements.
  - Don't Share Too Much Information With Charities

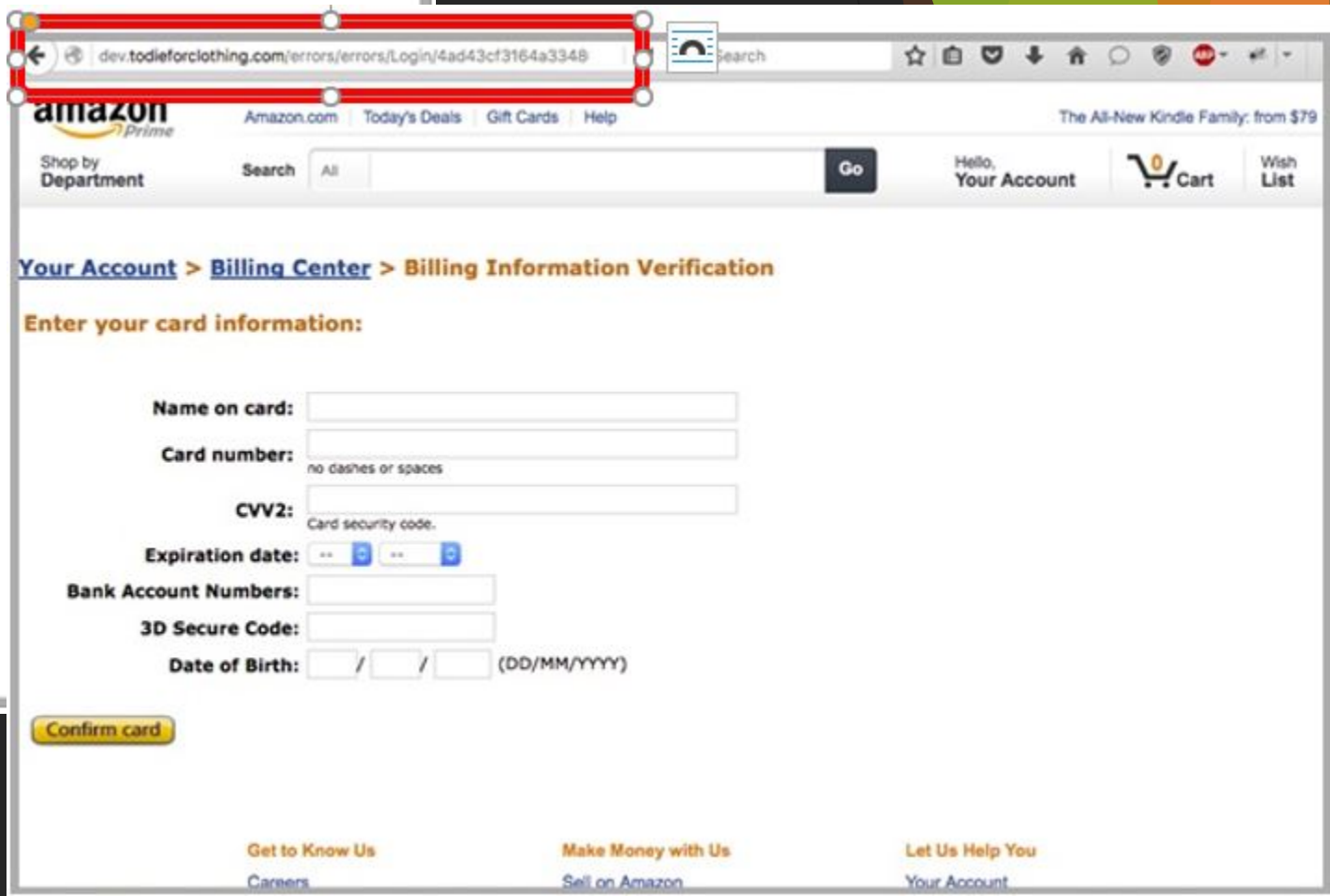
Email Attacks - Spoofing





Email Attack- Spoofing





Social Engineering

Social engineering attacks happen in one or more steps.

A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Social Engineering

What Does a Social Engineering Attack Look Like?

Email from a friend: Manages to hack or socially engineer one person's email password they have access to that person's contact list–and because most people use one password everywhere, they probably have access to that person's social networking contacts as well.

Using a compelling story or pretext, these messages may:

- Using a compelling story or pretext, these messages may:
- Use phishing attempts with a legitimate-seeming background
- Ask you to donate to their charitable fundraiser, or some other cause.
- Present a problem that requires you to "verify" your information by clicking on a link
- Pose as a boss or coworker.

Social Engineering

Don't become a victim

Tips to Remember:

- Slow down.
- Research the facts
- Don't let a link be in control of where you land
- Beware of any download.
- Foreign offers are fake.

Ways to Protect Yourself

- Delete any request for financial information or passwords
- Reject requests for help or offers of help.
- Set your spam filters to high
- Secure your computing devices

Ransomware

Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.

In 2021, the largest ransomware payout was made by an insurance company at $40 million (Business Insider 2021)

The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020 & $570,000 in the first half of 2021 (PaloAlto)

The average downtime a company experiences after a ransomware attack is 21 days. (Coveware, 2021)

Ransomware - Statistics

Survey conducted with 1,263 companies, 80% of victims who submitted a ransom payment experienced another attack soon after, and 46% got access to their data but most of it was corrupted. (Cybereason, 2021)

Additionally, 60% of survey respondents experienced revenue loss and 53% stated their brands were damaged as a result. (Cybereason, 2021)

42% of companies with cyber insurance policies in place indicated that insurance only covered a small part of damages resulting from a ransomware attack. (Cybereason, 2021)

Ransomware -Healthcare

Healthcare organizations dedicate only around 6% of their budget to cybersecurity measures. (Fierce Healthcare, 2020)

Ransomware attacks were responsible for almost 50% of all healthcare data breaches in 2020. (**Health and Human Services**, 2021)

September 2020 alone, cybercriminals infiltrated and stole 9.7 million medical records. (**HIPAA Journal**, 2020)

In 2020, 560 healthcare facilities were affected by ransomware attacks in 80 separate incidents. (Emsisoft, 2021)

Ransomware – Financial Industry

There's a rising threat to small financial institutions with less than $35 million in revenue.)(**National Credit Union Administration**)

LokiBot has targeted over 100 financial institutions, getting away with more than $2 million in revenue. (**Hub Security**, 2021)

Banks experienced a 520% increase in phishing and ransomware attempts between March and June in 2020. (**American Banker**, 2020)

Ransomware - Prevention

- Security Training
- Avoid Clicking on Suspicious Links
- Use Email and Endpoint protections
- Stronger Password System
- Employee Access Control Management
- Implement Zero Trust Security Model
- Keep Immutable, Offsite Back up

Myths about Cybersecurity

- Risks are well-known.
- Cybercriminals are outsiders.
- My industry is safe.
- Cybercriminals don't target small or medium-sized businesses
- We've never experienced a cyberattack, so our security posture must be strong enough
- Our passwords are strong enough to avoid a data breach
- Anti-virus and anti-malware software are enough to keep us safe:
- IT department is responsible for cybersecurity:

Cyber Hygiene - Personal

- Managing Your Privacy Settings
- Raising Privacy-Savvy Kids
- Personal Information Is Like Money. Value It. Protect It.
  - Know what's being collected, who is collecting it and how it will be used
- Own your online presence
- Configure 3 Wi-Fi access at home for
  1. TV & IoT,
  2. PC & Laptop Use
  3. Friends & Visitors
- Create Separate email for Rewards and newsletter
- Be conscious when downloading Apps/games on your phone and Tablet

Cyber Hygiene – Work

- Update all software or hardware that have updates available.
- Ensure antivirus and antimalware software is properly installed and configured.
- Ensure proper password management.
- Limit those who have administrative access to the network.
- Keep your hard drive clean
- Back up regularly
- Use multi-factor authentication
- Set strong passwords
- Use network firewalls
- Make sure routers and firewalls are properly set up and configured.

Review

- Statistics
- Finance & Banking
- Email Hijacking
- Social Engineering
- Ransomware –
- Myths about Cybersecurity
- Cyber Hygiene

Questions