Ransomware, Phishing & Cyberattacks

Craig Williams, Speaker
- Director Infrastructure Consulting Services, ClientFirst Technology Consulting
Email: cwilliams@clientfirstcg.com
Mobile: 630.656.7366

CLIENTFIRST TECHNOLOGY CONSULTING

Security Incident

Do you use the same password for multiple accounts?

- Never use the same password for more than one account. After a data breach, hackers will try user/pass combos on popular sites. Also make sure you are using strong passwords that you change regularly!

Do you hover your mouse over links and see where they go?

- Always hover over hyperlinks to make sure they go where you expect. When in doubt, go directly to the source rather than clicking on an unknown link.

Do you open email attachments from people you do not know or didn't expect or ask for?

- Be cautious with unknown emails. Verify the sender by another means before taking any action.
- Malicious attachments are a well-known phishing infection vector. Check with the sender before opening!

supportCon

Do you reply to emails that are unusual or out of character?

- The sender could have had their domain spoofed. Check with them in person or via phone first, better to be safe than sorry.

Do you transfer money to friends that were mugged abroad?

- By now this is a well-known scam, but the message is always evolving. Phishing emails often ask you to act with a sense of urgency, hoping you'll click without thinking.

Do you respond to emails that say you've won the sweepstakes?

- Whether it's a sweepstakes or some other lavish prize, phishing emails often sound too good to be true.

Connected Society

- The average adult maintains five social media accounts, three separate emails, and over fifteen various internet-connected services.

Threats

- Phishing
- Spoofing
- SMiShing
- Viruses/Spyware
- Ransomware

Threat Definitions

Spyware

Spyware monitors activity or harvests data without your knowledge.

This type of malware is used to gain information.

Advanced Persistent Threat

APT is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.

Ransomware

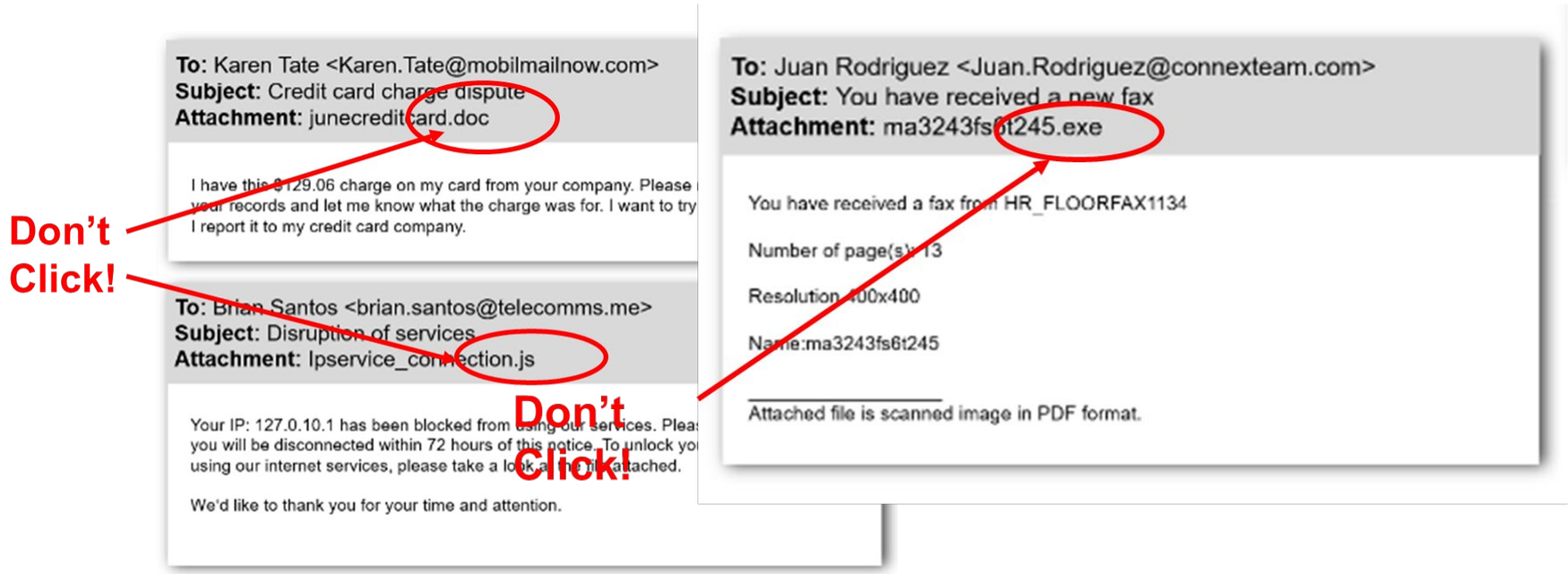
Ransomware restricts access to a computer or set of files until a ransom is paid to the attacker.

Viruses/Spyware/Ransomware

- Protection at the firewall
- Prevent executable attachments
  - Check with your IT
- Don’t click, allow access, or run if unsure or unsolicited

Ransomware - Attachments

- Over 68% of Ransomware are these file types:



Ransomware Protections

- Avoid peer-to-peer file sharing
- Stick to sites you trust
- Use caution around links
- Bookmark your favorite sites
- Don’t download strange attachments – know the source!
- Avoid scripts and executables
- Never enable macros

Social Engineering

- Attacker uses human interaction (social skills)
- Engages in dialogue
- Encourages clicking to other links

Phishing

- Form of Social Engineering
- Posing as trustworthy organization
- Take advantage of current events and certain times of the year

Phishing Example

From: Microsoft@apcprd01.prod.exchangelabs.com [mailto:Microsoft@apcprd01.prod.exchangelabs.com]
Sent: Thursday, October 19, 2017 9:25 AM
To: Tom Jakobsen <tjakobsen@clientfirstcg.com>
Subject: Your password has been compromised

Microsoft Office

Hi Tjakobsen,

You received this message to notify you that your account tjakobsen@clientfirstcg.com will be deleted in few hours.

Due to System error CODE: MSO OZ893W found, An action is required kindly make use of the below button.

RECENT ACTIVITIES

Phishing Example

- From: american express <welcome91cfkwq3qnfl25srbxw@forusprotecti7.com>
  To: undisclosed-recipients:;
  Sent: Tue, Dec 19, 2017 12:27 pm
  Subject: Reminder - Problem About Your Membership.
- There's been activity in your American Express account that seems unusual compared to your normal account activities on Tuesday, December 19, 2017

  (Please fill all necessary data which is asked in the verification page, it's important for us to verify you are the true owner)

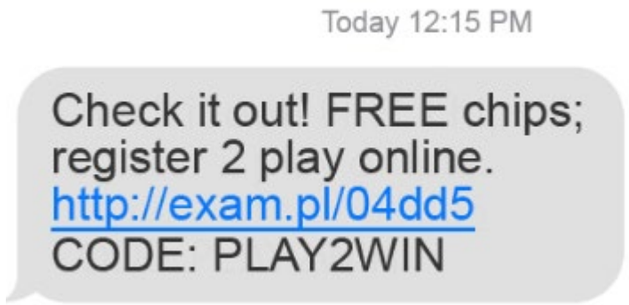
  Read your secure message by opening the attachment (Confirmation36591Membership.pdf) you will be prompted to open (Confirm Account) the file or save (download) it to your computer. for best results, save the file first, then open it in a Web browser.

  Sincerely,

  American Express Membership Group.
-

SMiShing

- Phishing via SMS text message:



SMiShing

- Phishing Messages
  - Attackers are sending shorter messages to accommodate screen size
- Application Stores
  - Be aware of copycat applications from third-party developers
  - Only download applications from trusted sources
- Pre-Installed on Devices
  - Malware has been found on new genetic-type tablets that have been sold through online retailers. The pre-loaded malware is designed to install adware and hijack search results.

Safe Mobile Computing

- Protect mobile devices:
- Passwords!
- Turn off blue tooth or wireless when not in use
- Be careful when downloading Apps!
- Leave Location Tracking off
- Be careful when connecting to open wireless networks
- Make sure you can track the device if it’s lost

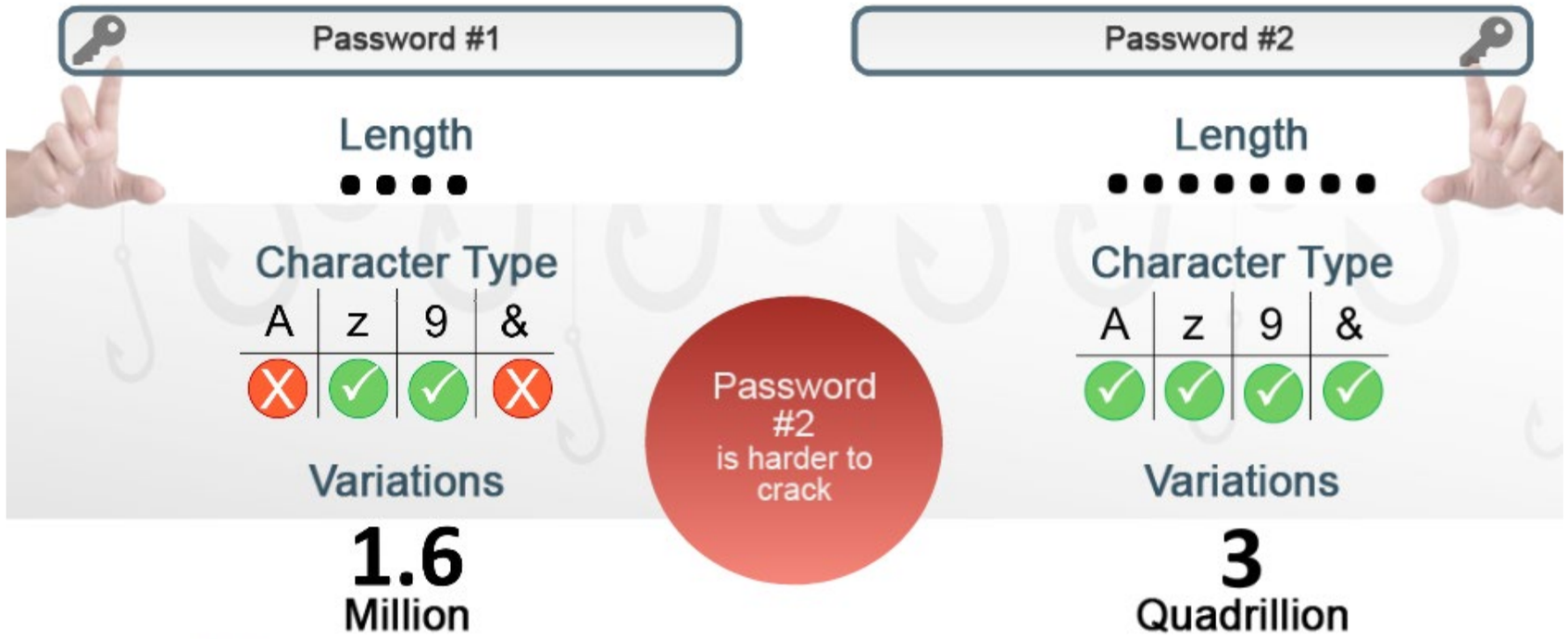
Avoid Being a Victim

- Be suspicious of unsolicited contact
- Be cautious when providing personal information o information about your district
- Do not revel personal or financial information in email
- Pay attention to email addresses and website addresses

Strong Passwords

- Avoid using
  - Personal information
  - Dictionary words
- Use
  - Mnemonics
  - Upper- and lower-case letters
  - Punctuation and numbers

What Makes a Strong Password?



Compromised?

- Changes in normal account activity
- Failure to receive regular bills or mail
- Not able to log in to normal websites

What To Do If Stolen

- Change passwords (use strong passwords)
- Go to identitytheft.gov for one-stop resource
- Contact companies you have accounts at
- Contact Police

Links To More Info

- www.haveibeenpwned.com – see if your email has been compromised in a data breach
- www.IdentityTheft.gov – government site with resources to report and recover from identity theft
- phishingquiz.withgoogle.com – site with phishing quiz sponsored by Google
- www.cnet.com/news/best-password-managers-for-2019 - LastPass (free), 1Password (paid), and others reviewed

Questions and Answers

We thank you for your time!