Computer and E-mail Security in a COVID-19 World

Jan L. Peterson (KD7ZWV)

Murray Amateur Radio Club

What Happened?

- Connie's e-mail got hacked
  - she had over a thousand contacts
  - the hacker copied her contacts and then deleted them all
  - the hacker also deleted all her mail from her account
  - the hacker created a new e-mail account on gmail that looked like it was Connie's
  - the hacker e-mailed all of Connie's contacts from this new account, asking for $200 worth of Amazon gift cards
  - several people called her to check if it was legit, but at least one person sent Amazon gift cards to the hacker
- Connie created a new e-mail account on gmail, but has been having a time trying to recover her contact list

How did it happen?

- Connie probably had an easy to guess password
- Connie could have had a virus on her computer that logged her keystrokes

How can I Protect Myself?

- Pick a good password (more on this in a minute)
- Don’t use the same password on multiple sites
- Don’t click on links that people send to you until you validate them
- Don’t download software/files from sites that you don’t trust
- If you get an e-mail from someone, and it looks weird, confirm that it is valid
  - double-check that the e-mail it is from is the one you know is theirs
  - call/text them to confirm
- Run anti-virus/anti-malware software
- Back up your files/contacts/etc.

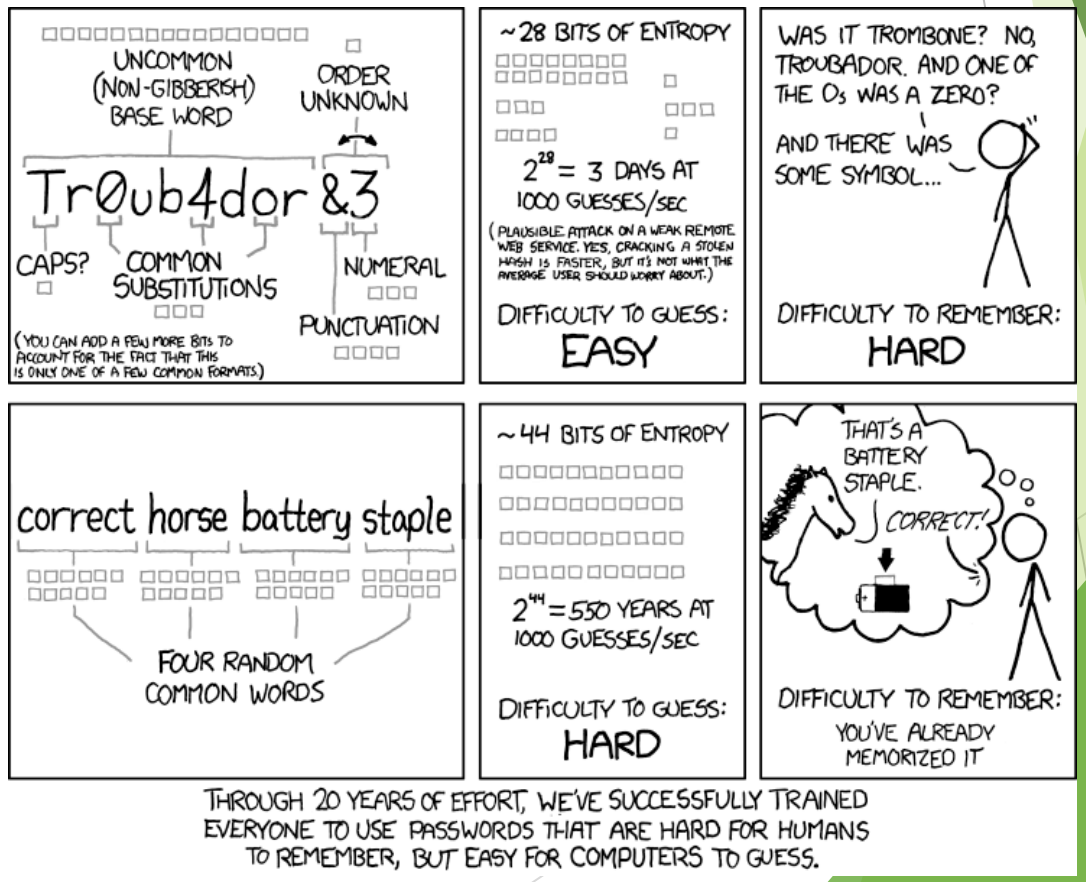
Let's Talk Passwords

- How do I pick a good password? What *is* a good password?
- STIG – Security Technology Implementation Guidelines
  - Minimum characters: 15
  - Minimum numbers: 1
  - Minimum lowercase characters: 1
  - Minimum uppercase characters: 1
  - Maximum consecutive repeating characters: 2
  - The last seven passwords cannot be reused

  - Example: 3loon7UnBate84p
  - Cons: hard to remember

Let's Talk Passwords

- How do I pick a good password? What ***is*** a good password?
- XKCD model: https://xkcd.com/936/
  - pick four random common words
  - Example:
    correct horse battery staple
  - Cons: a lot of sites want you to use more "complex" passwords, include digits/punctuation, etc.



Let's Talk Passwords

- How do I pick a good password? What ***is*** a good password?
- Phrase model
  - Pick a short but memorable phrase
  - Take the first or second letter of each word
  - Insert a digit/capitalization in the phrase
  - Example: Now is the time for all good men to come to the aid of their party.
    Password: Nittfagmtcttaotp.
  - Cons: Takes a while to get used to

Let’s Talk Passwords

- How do I pick a good password? What ***is*** a good password?
- Random crap model
  - just throw some random mash of characters out there
  - Example: A]s%*pZmYzpa?U4N
  - Cons: memorize that! yeah, I didn’t think so

Let's Talk Passwords

- How do I pick a good password? What ***is*** a good password?
- Combination of the above
  - pick some random words
  - inject some capital letters
  - inject some digits and/or punctuation

  - Example: 4ethnic-Bedim-Clam2-Deli-4lawns-magog
  - Cons: I'm sure there are some, but this is the mechanism I use

Password Usage

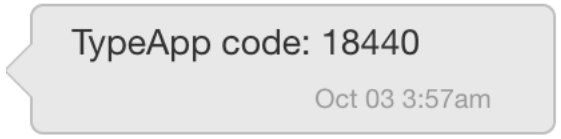
- NEVER use the same password for more than one site
- NEVER use the same password for more than one site
- NEVER use the same password for more than one site
- NEVER use the same password for more than one site
- NEVER use the same password for more than one site
- NEVER use the same password for more than one site
- NEVER use the same password for more than one site
- NEVER use the same password for more than one site
- NEVER use the same password for more than one site

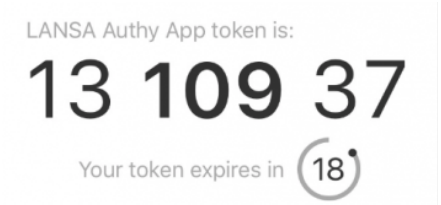
How do I Remember all Those Passwords?

- Use some kind of “password manager” software
- Many browsers have this built in (Chrome, Firefox, etc.)
- Some operating systems have this built in (MacOS “Keychain”, Linux “Keyring”, Windows “Credentials Manager”)
- Third party software https://www.pcmag.com/picks/the-best-password-managers
  - Lastpass
  - Enpass <- this is the one I use
  - Dashlane
  - 1password
  - etc. etc. etc.

Two-Factor Authentication

- Many web sites and cloud services offer “two-factor authentication”
- The two factors are typically “something you know” and “something you have”
- This typically involves the use of “one time” passwords or having the site send you a text message or e-mail to validate your login
- Examples include RSA SecurID tokens, TOTP systems like Authy



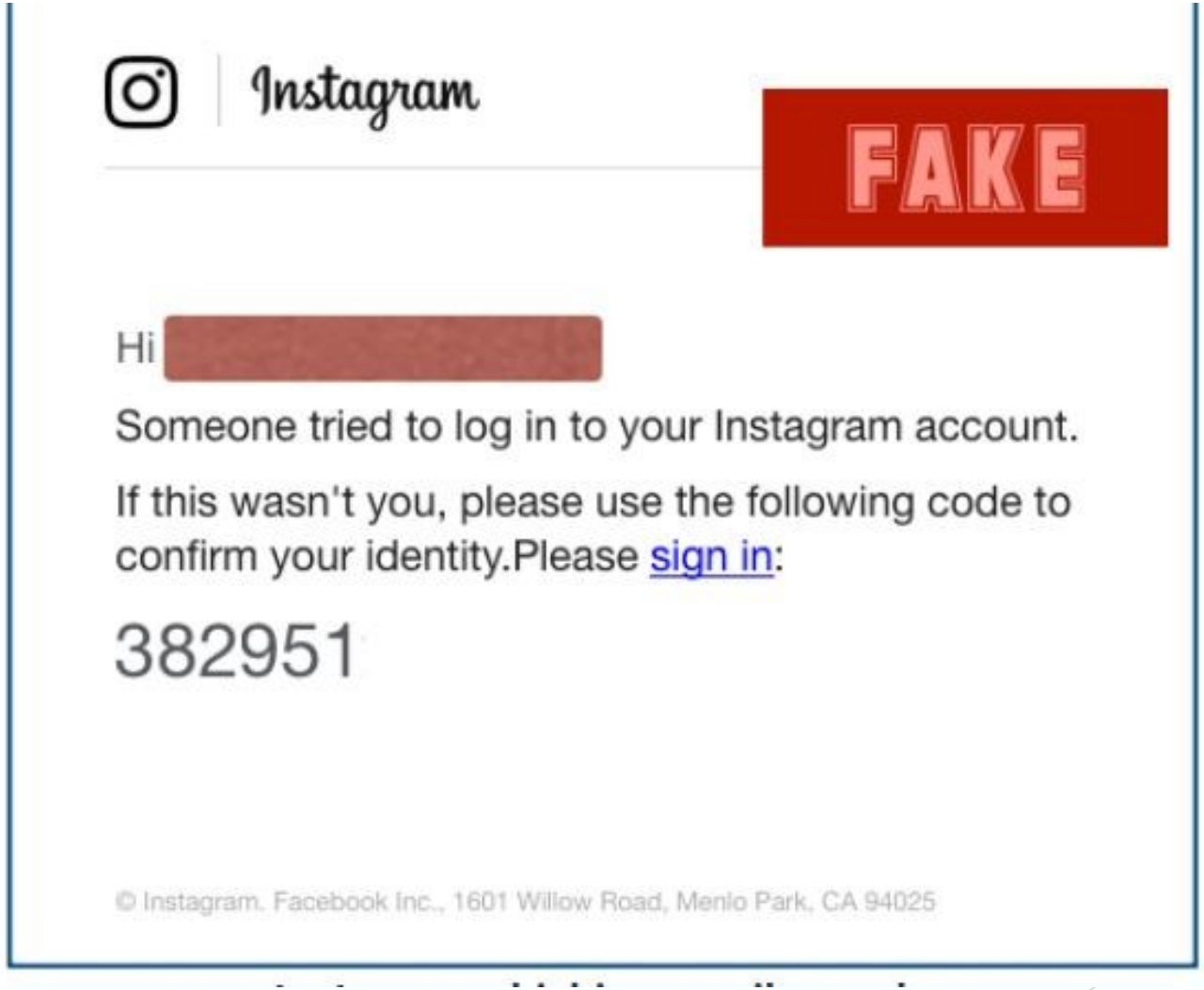


What is “Phishing”?

- An attempt to “fake you out” and get you to give someone your credentials
- Usually an e-mail that looks like it came from e.g. your bank, eBay, Facebook, etc.
- Tells you something that tries to encourage you to click on a link in the mail
- Clicking on the link takes you to a page that looks like the real site
- You log in and you’ve just given your username and password to them!

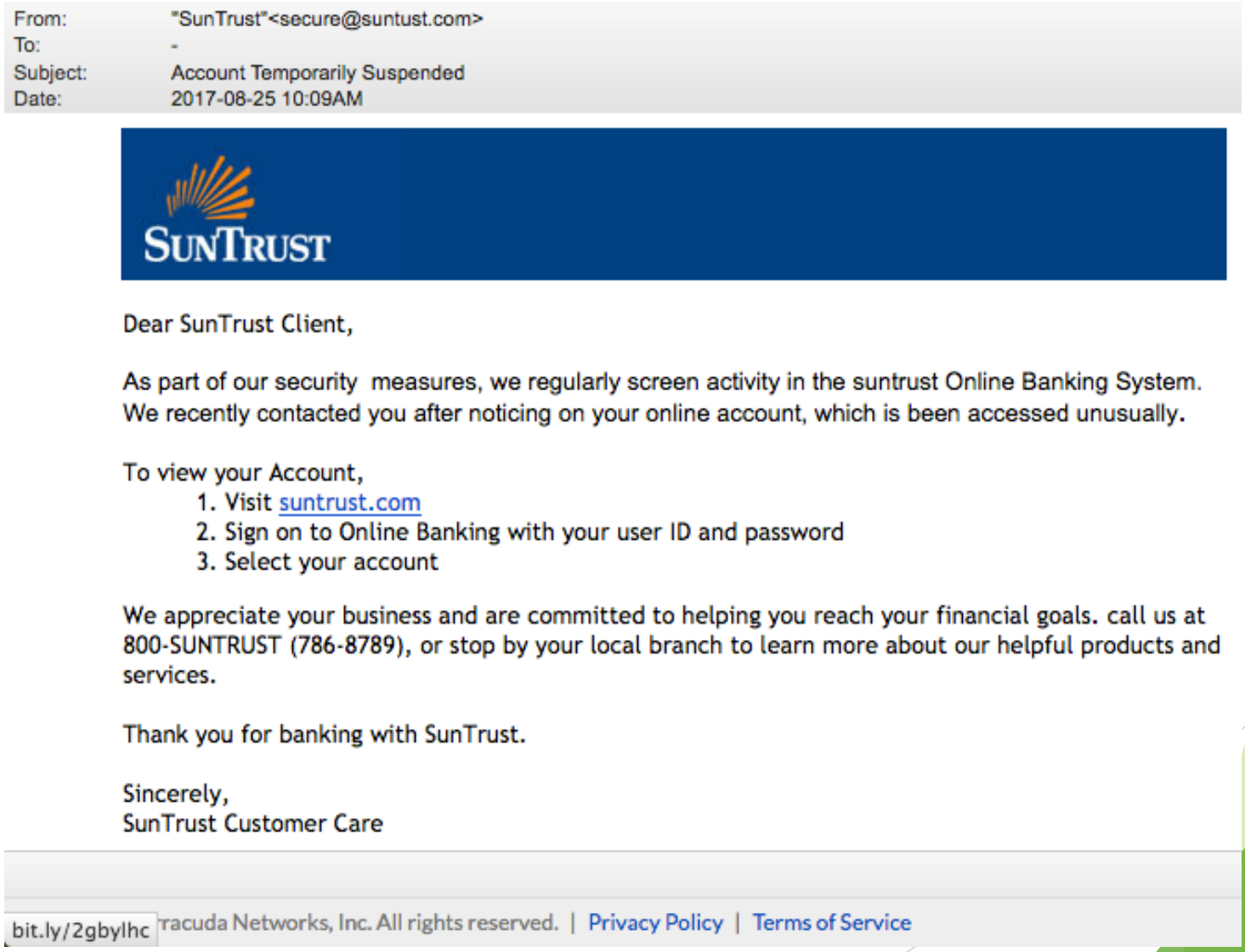
What is “Phishing”?

- Example:



What is “Phishing”?

- Example:



From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM

SUNTRUST

Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

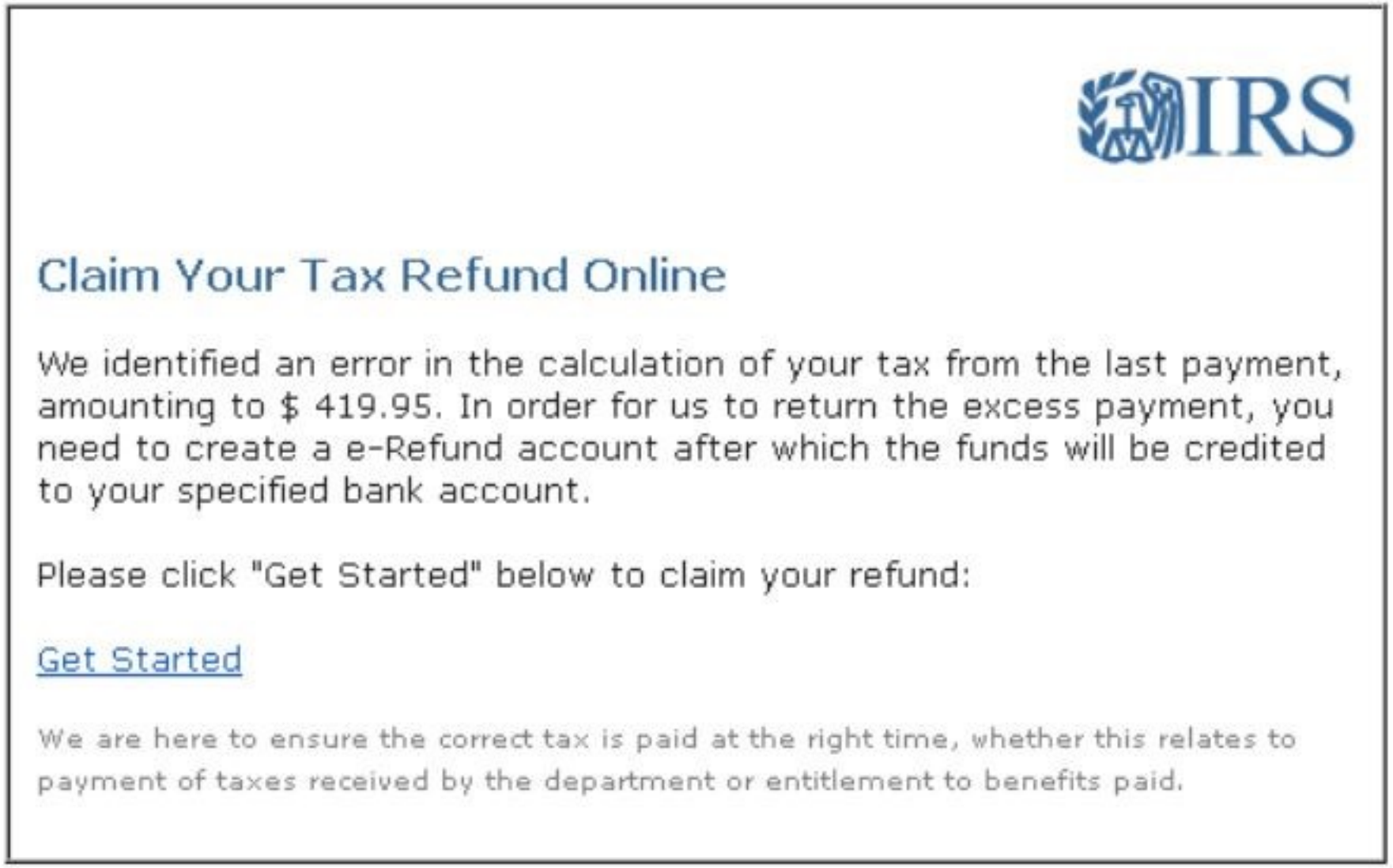
Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

bit.ly/2gbylhc racuda Networks, Inc. All rights reserved. | Privacy Policy | Terms of Service

What is “Phishing”?

- Example:

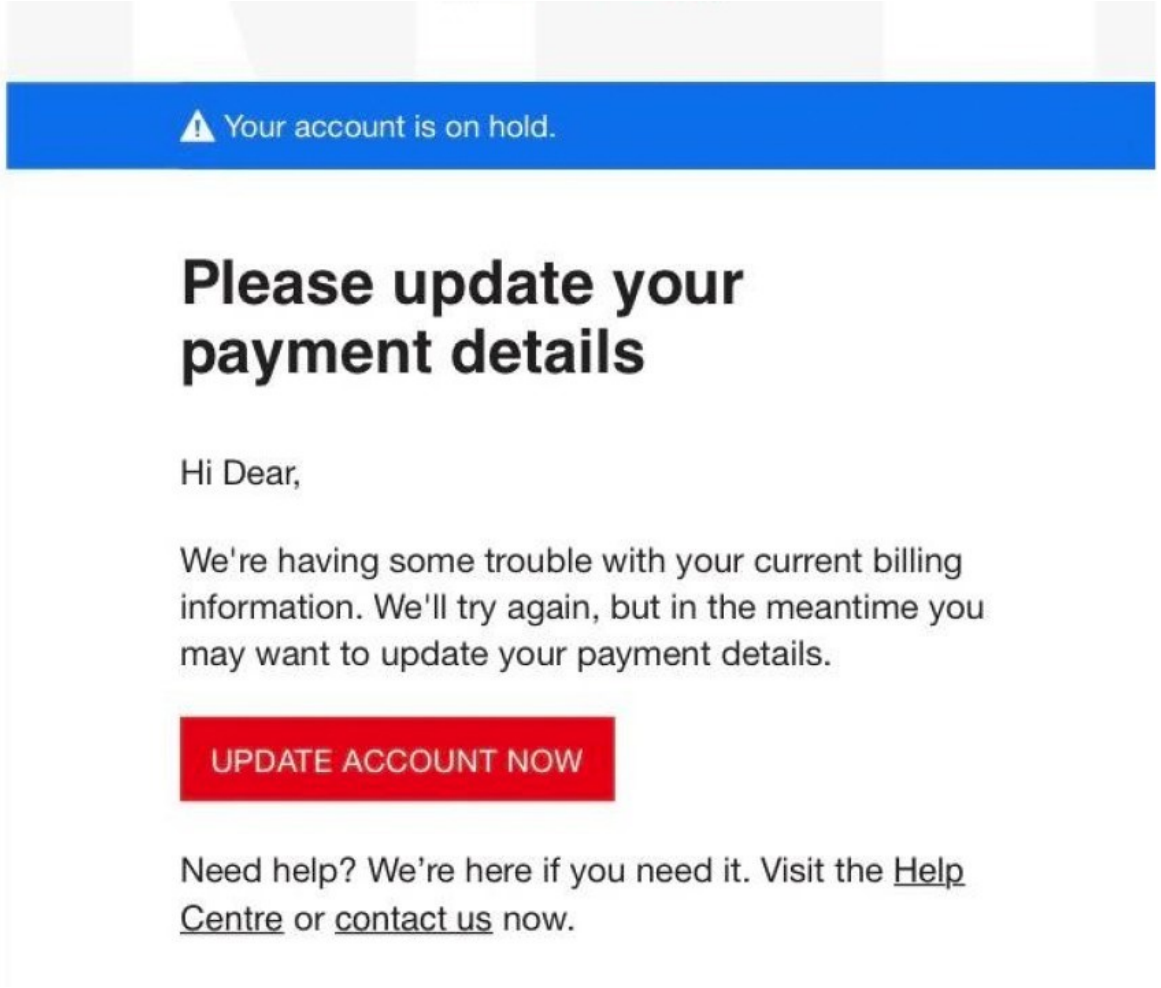


What is “Phishing”?

- Example:

What is “Phishing”?

- Example:



How to Recognize “Phishing”?

- Grammatical errors (word choice, punctuation, weird phrasing)
- Low resolution logo
- URL doesn’t go to the right site
- Tries to frighten you (your card is disabled, your order has been placed, etc.)
- E-mail is unexpected (you won a prize from a contest you don’t remember entering, you’re getting a refund that you weren’t expecting)
- Presumes to know something or someone that you know

- This is what Connie’s attacker tried to use against her contacts

Viruses, Trojans, Worms, and other Malware

- Viruses
- Trojans
- Worms
- Spyware
- Adware
- Ransomware
- Botnet

Viruses

- No, we're not talking about COVID-19
- Computer software that infiltrates "good" software and does something bad
- Replicates itself by inserting it's code into other programs
- Often used to transport/infect with some other type of malware
- Often take advantage of buggy software

Trojans

- Think of the story of the Trojan Horse
- YOU LET IT IN!
- Maybe you clicked on a link, downloaded some software and ran it, downloaded a video file that was really an executable, etc.
- Attack vector for other malware

Worms

- Type of malware that attempts to spread by exploiting vulnerabilities on other machines on your network
- Attempts to automatically spread from machine to machine
- Famous example, the Morris Internet Worm
  - November 2nd, 1988, Robert Morris at Cornell activated it using systems at MIT
  - Took advantage of known bugs in sendmail, finger, rsh, and poor passwords
  - Had a bug in it that made it easy to detect by it's side effects
  - Systems admins actually contacted the CDC to track and eradicate it
  - Spawned several security/vulnerability tracking systems/groups (CERT, etc.)

Spyware

- Type of malicious software that tracks what you are doing
- Monitors your keystrokes
- Takes screen captures
- Can activate your camera/microphone
- Records web sites you visit
- Logs your usernames/passwords

Adware

- Pops up advertisements on your computer
- Replaces legitimate ads on sites you are visiting with it's own
- Clicks on those ads can result in further malware infection
- Ads may encourage you to e.g. "run this anti-virus software" (which is really malware itself)

Ransomware

- Once it gets on your machine, it quietly and transparently encrypts your files
- Once your files are all encrypted, it blocks you from accessing your data
- It informs you that you have to pay to get your files back
- Often can affect your backups as well as it will usually wait a while before blocking you
- Because files are encrypted with strong crypto software, it is nearly impossible to decrypt them without the key
- Even if you pay the ransom, there is no guarantee that the software won't keep doing its thing and come back at you later for another round

Botnet

- Quietly sits on your computer waiting for instructions
- Can use your computer to instigate an attack (typically called a “denial of service” attack) on some victim
- Since millions of computers around the world are infected, it is hard to impossible to stop

How do I Protect Myself from Malware?

- Get and run some good antivirus/antimalware software
- https://www.malwarebytes.com/mwb-download/
- Free for personal use!
- Works on Windows, MacOS, Android, and iOS

- Install OS updates when offered

- Linux users can run ClamAV

I use Linux/Unix, am I safe?

- NO
  - Linux viruses are now being made
  - You are still vulnerable to phishing attacks
  - Windows viruses on your Linux machine could attack other systems on your home network
- The Morris worm specifically targeted Unix and Unix-like systems
- Keep your system updated
- Upgrade when your OS is no longer supported (e.g. Ubuntu 16.04 LTS will end support on April 30th 2021, upgrade before that happens!)

Backups

- Are your files/e-mails on your computer/Internet important to you?
  - Financial documents (taxes, bank statements, mortgage info, credit cards, etc.)
  - Medical information (insurance claims, doctor visit notes, test results)
  - Family photos and videos
  - Contact lists (personal and professional)
  - E-mail history (records of conversations, documents, etc.)
  - Account information (cell phone, internet service, Facebook, Twitter, etc.)

Backups

- Copy important files to multiple storage devices/locations
  - Floppy disks (ha ha ha)
  - USB drives
  - CD/DVD-RW
  - Backup hard drives
  - NAS (Asustor, Synology, TerraMaster)
  - Cloud storage (OneDrive, iCloud, Google Drive, Dropbox)
  - Commercial storage options (Amazon S3, Backblaze, Carbonite (formerly Mozy))

Backup Strategies

- Daily/Weekly/Monthly schedule
- Store a copy off site (in the cloud, at your kid's house, etc.)
- Automate it!
- Test it (try to restore a file every once in a while)
- Don't forget to back up your e-mail and contacts

I’ve Been Hacked, Now What?

When in Trouble or in Doubt
Run in circles, scream and shout!

I’ve Been Hacked, Now What?

- Disconnect your computer from the network
- Use another computer to change your passwords
  - First, change your e-mail password... all your other services will send password update requests to your e-mail, so secure that first
  - Second, change any financial account passwords, your bank, your mortgage, your credit cards... have them cancel your cards and issue new ones at this time
  - Third, change other passwords for commercial services where you may have payment information stored (Amazon, eBay, your ISP, even sites you wouldn’t think about like Walmart.com, the restaurant you order from online, etc.)
  - Fourth, social media and other accounts
- If you suspect any fraudulent activity, contact the police and file a report

I’ve Been Hacked, Now What?

- Notify your contacts that you were hacked and that they should be suspicious of any e-mails that came from you recently
- Contact the three major credit bureaus (Equifax, Experian, and TransUnion) and explain that you are a victim of identity theft... they have special procedures to help with this
- Boot your computer from secure media and run anti-malware software against it (if you don’t feel comfortable doing this, take it down to PC Laptops, they will scan your machine for free)
- Consider wiping your computer and re-installing from known good media (and getting your files back from your backups... you have backups, now, right?)

Q&A and References

- https://www.pcmag.com/picks/the-best-password-managers
- https://us.norton.com/internetsecurity-online-scams-phishing-email-examples.html
- https://en.wikipedia.org/wiki/Morris_worm
- https://www.malwarebytes.com/mwb-download/
- https://www.safetydetectives.com/blog/best-really-free-antivirus-for-linux/
- https://www.pcmag.com/picks/the-best-nas-network-attached-storage-devices
- https://www.vox.com/2014/9/11/11630774/what-to-do-if-youve-been-hacked-and-how-to-prevent-it
- https://pthree.org/2018/04/19/use-a-good-password-generator/