Cyber Security for Leadership

Presented by Jeremy Paulson, CISSP
Cyber Security Coordinator
Community Security Initiative

COMMUNITY SECURITY INITIATIVE

A JOINT PROGRAM OF

UJA Federation NEW YORK

jcrc

What Are the Risks?

What Are Cyber Risks?

- Damage to Operations.
- Loss of Data.
- Disclosure of Privileged Information.
- Web Defacement.

Dealing with the Jargon (There's lots of it!)

- Attack Surface: Any point where infiltration may occur.
- Attack Vector: The actual cyber attack.
- Firewall: a Hardware device or software program that monitors outgoing and incoming data. It also enforces white lists and black lists, limiting communication to authorized or avoiding bad web addresses.
- Endpoint Protection: What we used to call anti-virus software, now with advanced detection and recovery capabilities.

What are the Bad Guys doing?

- Website Defacement
- Phishing, Vishing, Spear Phishing and Social Engineering
- Trusted Source Impersonation
- “Man in the Middle attacks”
- Malware Injection

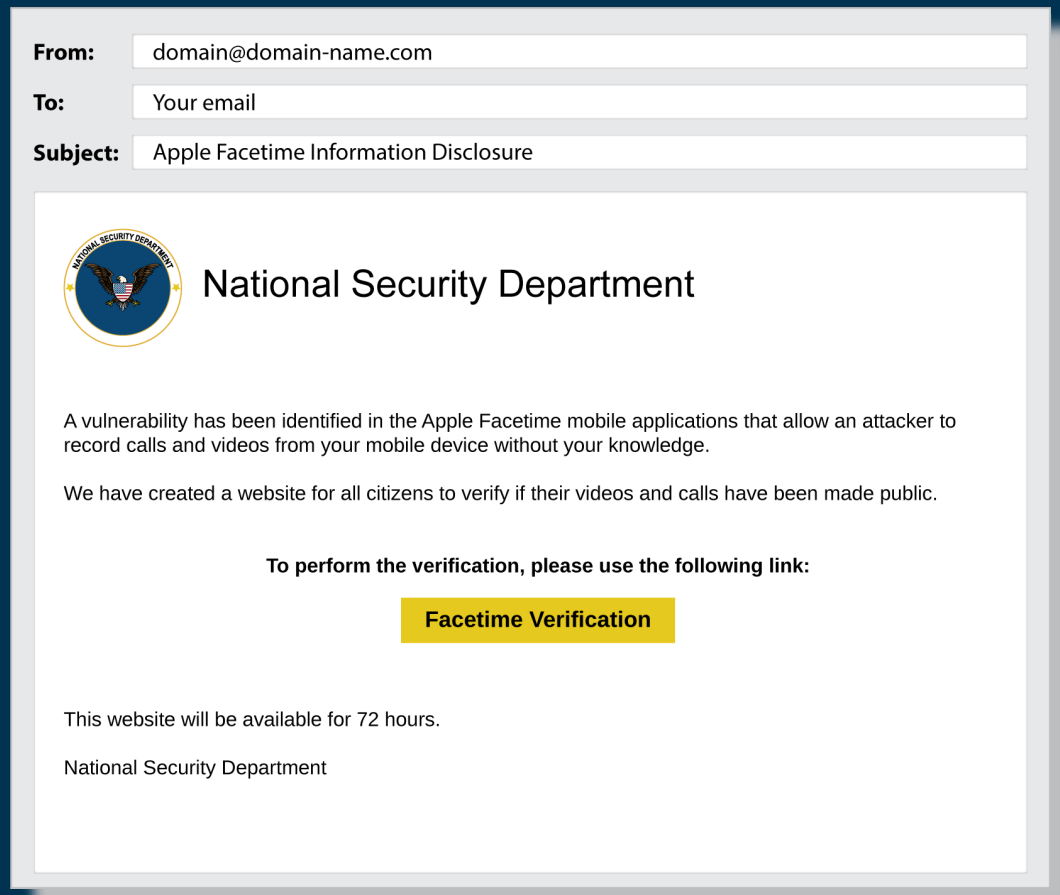
Typical Attack Types

- Phishing, Vishing, Spear Phishing, and Social Engineering: the distribution of emails with the intent to direct the target to enable theft of money, data, and/or credentials.
- Trusted Source Impersonation: Where a trusted source directs someone to transfer money or provide access to the network.
- Malware: Generally, any code designed to have a negative effect on your network. This may include: data destruction, process damage, exfiltration of data, and ransomware.
- Ransomware: Malware designed to infect a network and encrypt all data on the network. The encryption key necessary is offered for a fee.
- Distributed Denial of Service (DDoS): The process of overloading a network with so many call that it shuts down.
- Credential Attacks: Brute force attempts to guess passwords through multiple attempts.
- Escalation of Privileges: Once a hacker is in your system, they take control of an account and increase that accounts access to higher levels of access. The goal is to enable access to critical data.

Website Defacement

Used to damage communications or hinder operations.
Usually for ideological reasons.

Phishing attacks, including Spear Phishing, and Social Engineering



From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

- These are emails designed to drive you to a website that asks for personal information.
- The usual approach is to panic you into responding.
- Often these purport to be from the IRS, Social Security, or any service that is vital to you.

Phishing Attack: they say you won something

- If it looks too good to be true,
- IT IS!!

Trusted Source Impersonation

- A type of Social Engineering
- An apparently trusted source sends an email asking for the recipient to do something.
- It can vary from asking for funds to be transferred, to requesting credentials.
- Or it can ask that an attachment should be opened.

Vishing: an Audio or Video Phishing Attack

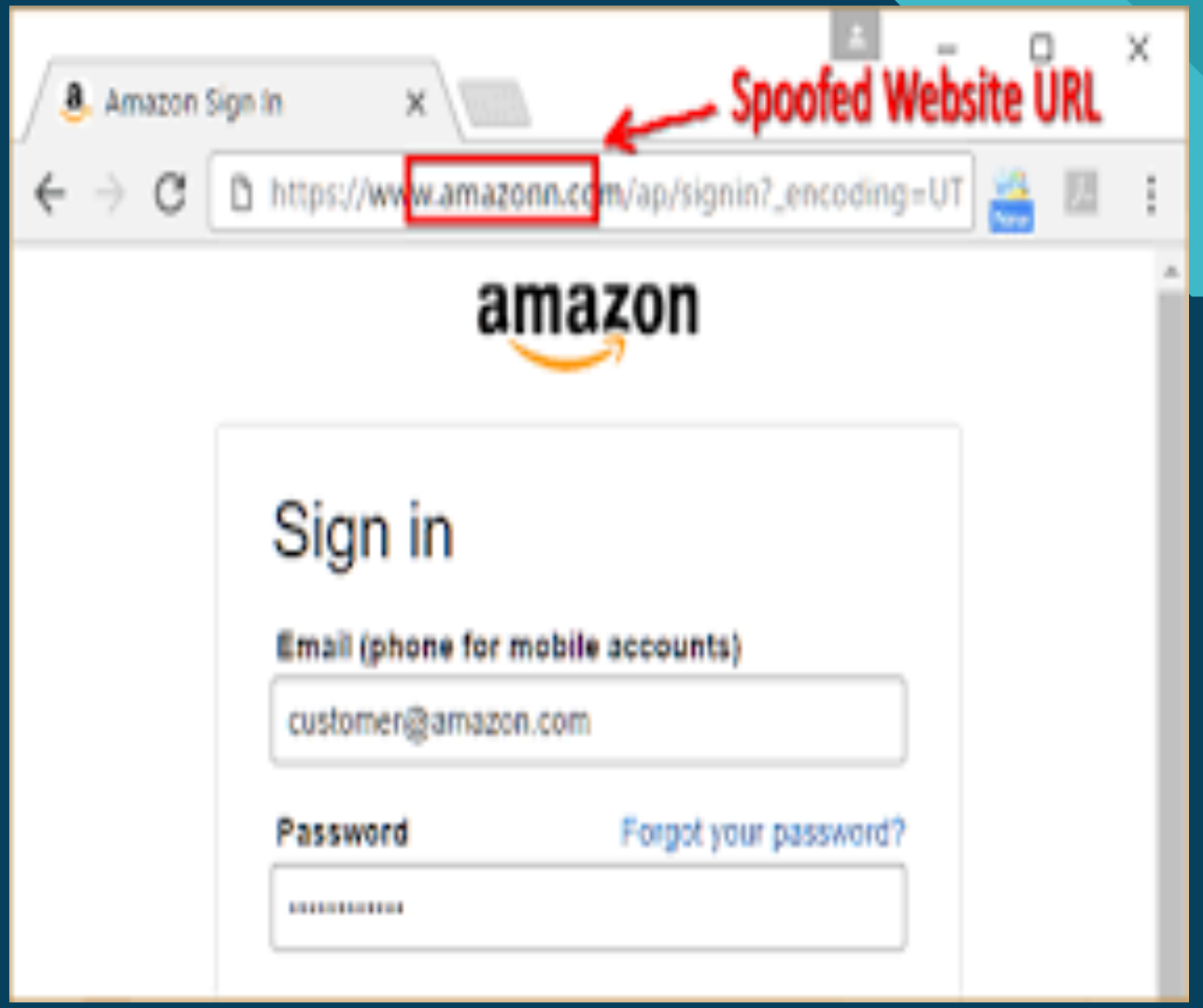
- The practice of making phone calls or leaving voice messages in order to get individuals to reveal personal information.
- Hackers can spoof caller ID to portray themselves as a trusted source.
- Voice technology can be used to mimic trusted individuals.

- Solution: Always verify requests for information with out of channel sources (your phone calls, emails, in person communication).

Points of Defense

- Router/Firewall: Monitors traffic incoming and outgoing. Also limits DDoS attacks.
- Backups: To protect against data loss and to recover from ransomware.
- Endpoint Protection: Monitors traffic for malware behavior. More advanced solutions isolate infected computers from the network. Stopping

Examples of Spoofed websites



Malware injection

- Goal: to damage operations, create “bot” computers, and steal data.
- Delivery Method: through emails, phishing, zero-day exploits, and fake websites.
- “Bot” computers are compromised so the bad actor can use the computer for things like DDoS attacks and crypto mining.
- Other malware types are Wiperware and Ransomware.

Wiperware

- A new “gift” from the Russian cyber attack teams.
- Method: a type of malware that wipes the boot records on computers.
- These boot records are vital to restarting the device.
- If the records are wiped the computer doesn’t know where files are that it needs to restart.
- Solution: Either a very expensive software rebuild of the hard drive file directory, or you need to reformat the hard drive. Thus, losing all data on the drive.

Ransomware

- What is it?
  - Malware that encrypts data followed up with a ransom note
  - Payment is made, usually through Bitcoin, to acquire the necessary encryption key to decrypt the locked data.
  - Prevalence:
    - “Experts anticipate a ransomware attack will happen every 11 seconds in 2021.” (Cybercrime Magazine 2019)
  - Objective: Profit

What you can do

- Update software and operating systems.
- Authentication: Move to multi-factor authentication (MFA)
- Backups: take them at least daily. Have two independent backups: one onsite, and one offsite.
- Endpoint Protection: Rely on advanced products that look for malicious behavior and can isolate infected computers from the rest of the network, stopping further infection.
- Cyber Security Training for Staff: To educate and increase awareness to malware injection, credential theft, and phishing attacks.

What We Do...

- Cyber Security Assessments: To identify vulnerabilities, solutions, and provide grant support.
- Cyber Security Newsletter: produced monthly to inform leadership of new risks and focus on critical aspects of cyber security.
- Cyber Security Training for Staff and Leadership
- Consultation Services: including (but not exclusively) ransomware recovery, product recommendations, and service providers.

Ransomware Example

What can you do?

- Use “Strong” Passwords
  - 8 characters including Upper Case, Lower Case, Numbers, and Special Characters (e.g., ~ $* %).
- Use Multi-factor authentication when and where available.
- Lower your online accessibility
  - Limit access to your social media posts to actual friends.
  - Avoid public posts.
- Restrict access to Personally Identifiable Information (PII).
- NEVER respond to unsolicited emails.
- Don’t open attachments to emails unless you KNOW the sender.
- When ordering online only use sites with “HTTPS” in the web address.
- Patch! Keep all software up to date.
- Avoid using non-employment devices to log into your employment network.
- Never save your work product to internet locations other than company devices or servers.

COMMUNITY SECURITY INITIATIVE

A JOINT PROGRAM OF UJA Federation NEW YORK jcrc

Thank You

COMMUNITY SECURITY INITIATIVE

A JOINT PROGRAM OF

UJA Federation NEW YORK

JCRC

Jeremy Paulson, MBA, CISSP
Cyber Security Coordinator
Community Security Initative
paulsonj@jcrcny.org

COMMUNITY SECURITY INITIATIVE

A JOINT PROGRAM OF

UJA Federation NEW YORK

jcrc