Cyber Security
Securing the Court

Kris Virtue

Carol Lam

Qualcomm

Cyber Attacks

Common Attack Types

Phishing

An email-based fraud with the objective of either:

- Obtaining the victim’s personal, financial, or company information
- Installing malware that allows the attacker remote access into the victim’s computer.

Malware

Malicious software intentionally designed to cause damage to a computer, server, or computer network.

Ransomware

Malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Denial of Service

An attack designed to render the computer network and systems unusable.

Denial of service attacks are usually temporary in nature.

OneIT

Attacks are always evolving

Attacker Types

	Nation States	Organized Criminals	Competitors & Entrepreneurs	Hacktivists	Rogue Insiders	Nuisance Actors
						
Objectives:	• Create economic or political advantage • Increase defense & intelligence capabilities	• Financial gain	• Financial gain • Technology gain • Market advantage	• Political and social statements	• Financial gain • Revenge	• Amusement • Experimentation • Ego/reputation building
Characteristics:	• Targeted • Very sophisticated • Diverse	• Targeted • Mixed sophistication • Diverse	• Targeted • Mixed sophistication • Diverse	• Targeted • Mixed sophistication • Diverse	• Targeted • Mixed sophistication • Diverse	• Random • Low sophistication • Noisy
Targets:	• Companies and people • Other nations • Own population	• Companies and individuals with resources	• Companies in competitive markets	• Entities on a different side of a political or social issue	• Companies or other entities they work at	• Anything on the Internet
Examples:	• Targeted cyber attacks to steal data or disrupt operations	• Targeted attacks to steal passwords and perform identity theft	• Stealing data from company systems and sharing with competitors	• Targeted attacks to disrupt and embarrass companies	• Stealing data from company systems for personal use • Sabotaging company systems with logic bombs	• Attacks on random computers to build botnets or spam servers

Cyber Attack Trends

Nation-State Attacks

- Motives include Mis-information, political targeting, destabilization and economic gain
- Russia, China, Iran, and North Korea routinely identified; however, smaller nation-states are also being named

Ransomware

- Ransomware doubled year-over-year in 2016 and 2017
- Attackers are targeting government agencies in addition to businesses, as they are more likely pay

Cryptocurrency Mining

- Multiple security firms have reported significant increases in cryptocurrency mining
- Some legitimate websites are publishing advertisements with crypto-mining

Internet of Things

- Hackers are turning their attention to routers, cameras, and other internet connected devices

Phishing

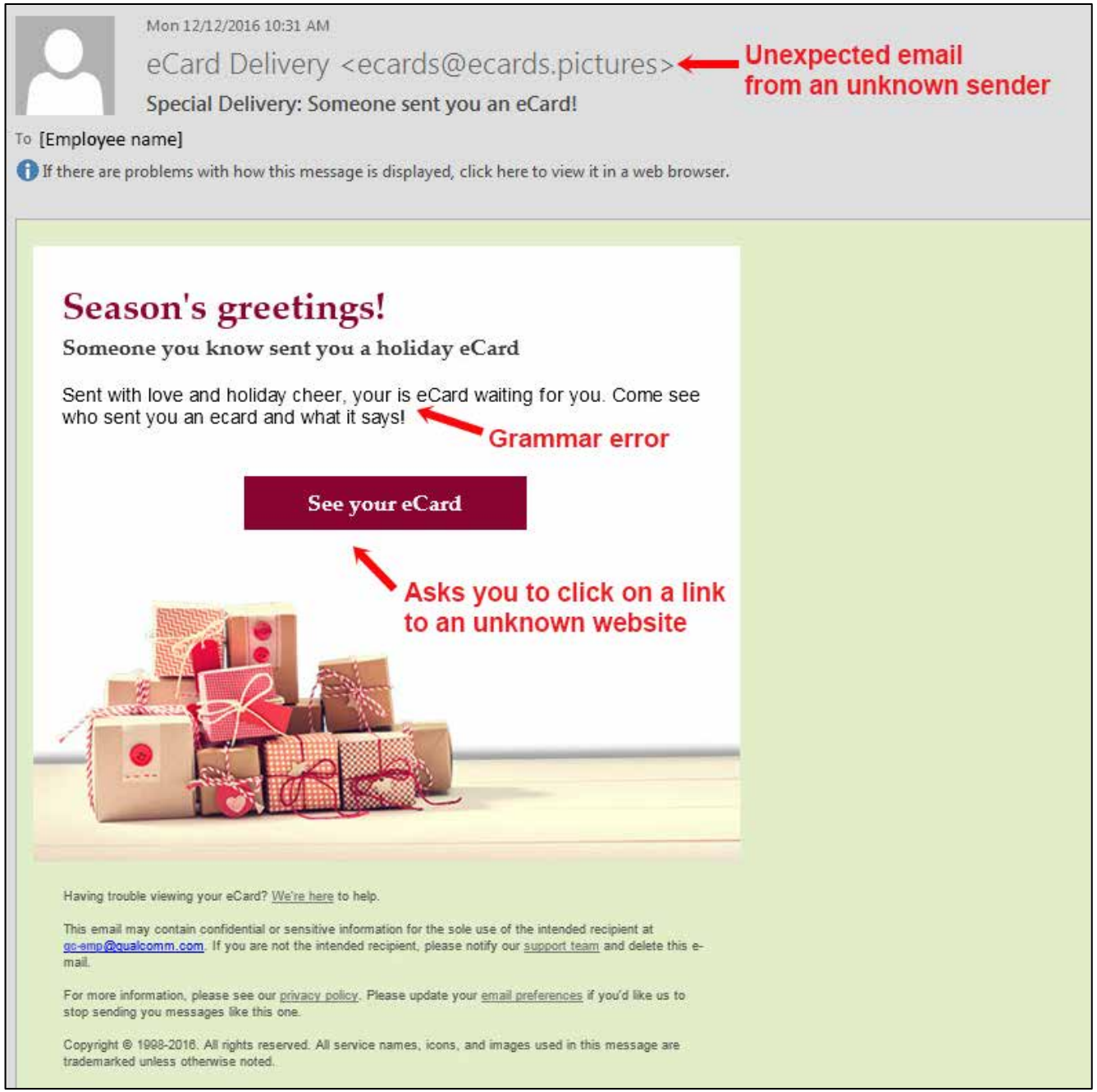
An email-based fraud that attempts to obtain information or install malware

- Phishing attacks are designed to appear legitimate. They **appear** to come from a trustworthy person or company.
- Telltale signs of a phishing attack:
  - The email is unexpected or comes from an unexpected sender.
    - Even when the message claims to come from someone you know, be suspicious if the contents are something the sender would typically not convey.
  - Asks you to click on a link, open an attachment, or provide sensitive information, such as account credentials, credit card number or other personal or confidential information.
  - Requests immediate action.
- How to respond to a suspected phishing attack:
  - **Don’t click on links or open attachments** in suspect emails.
    - Be especially concerned if you need to enable macros to view an attached document.
  - Don’t respond.

Phishing Example

Clues that this is a phishing attack

- The email is unexpected and comes from an unknown email address.
- The email creates a sense of urgency with the hope that you fall victim before the attack is discovered and blocked.
- The email asks you to click on a link.



Phishing Example

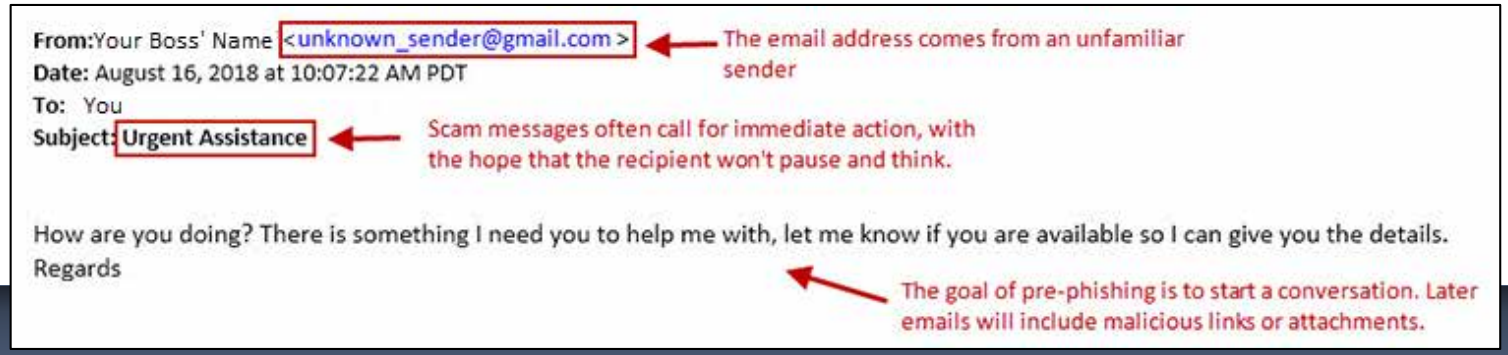
Clues that this is a phishing attack:

- The email is unexpected and comes from an unknown sender.
- The content of the email contains a grammar error, which should be unexpected from a commercial greeting card company.
- The email asks the recipient to click on a link that directs to an unfamiliar website.

Pre-Phishing and Spear Phishing

A longer-term sophisticated scam

- **Pre-phishing**
  - No malicious links, attachments or requests for sensitive information are included…yet.
- **Spear phishing**
  - May be spoofed to appear to come from someone the recipient knows.
  - Targets a specific person or group with a customized attack email.
  - May be personalized to include the recipient's name, company or other information.



The goal is to gain trust so that the recipient eventually provides sensitive information or installs malware

Ransomware

Ransomware is a type of malicious software that threatens to block access to the victim's data until a ransom is paid.

Ransomware In the News

A malicious software that locks you out of your computer until you pay a ransom

City of Atlanta

- Citizens turned away after cyberattack shuts down Atlanta Municipal Court
- Attackers requested $51,000 to unencrypt the computers, but the FBI advised against payment.
- The City of Atlanta paid over $3 million to remediate the attack.
- The Court's electronic case management system was restored **11 weeks** after the attack

UK National Health Service

- Ransomware impacted 45 hospital groups across the UK, bringing down key IT infrastructure that doctors and nursing staff use.
- Staff was forced to revert to pen and paper for providing medical services.
- Hospitals and doctors were forced to turn away patients and cancel appointments.

Maersk Transport & Logistics

- Impacted over 4,000 servers and 45,000 PCs.
- The company was forced to halt operations and had severe business disruption as a result of this attack.
- According to company estimates, the attack cost over $300 million.

Preventing and Remediating Ransomware

- **Prevent ransomware infections from occurring**:
  - Don’t click on links or open attachments in suspect emails. Most ransomware infections originate from a phishing attack.
  - Patch/update software and operating systems regularly.
  - Backup your important work. Keep the backups offline, disconnected from your system.
- **Ask your IT department the following:**
  - Is data backed up?
  - Are backups disconnected from the systems they’ve backed up?
  - What is the remediation plan if systems are unavailable?
- **To pay or to not pay?**
  - Paying ransom to criminals encourages them to continue attacks.
  - Even if a ransom is paid, the criminal may not release the files.

Password Safety

Passphrases

1. Create a sentence that's meaningful to you: e.g., The San Diego Chargers broke my heart.
2. Abbreviate, combine words, then add symbols and capitalization so that it becomes a passphrase: TheSDCHarGers_0_myhrt

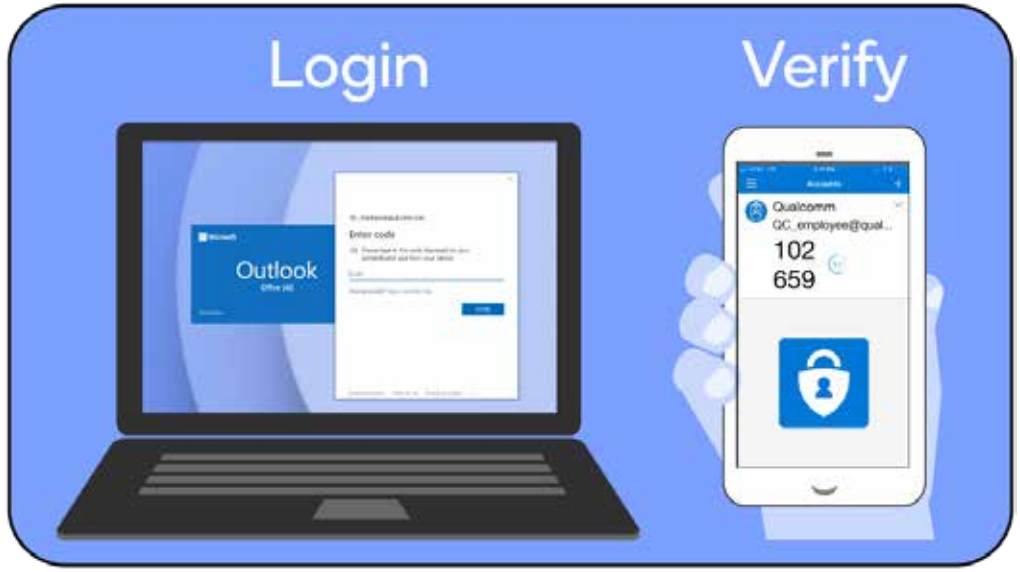
Four Random Words

1. String together four random words that don't make any grammatical or logical sense. e.g., stealthy photograph tooth moonbeam
2. abbreviate, combine, add symbols and capitalizations: stealthyfOtOgraft00thm**nbeam

Password Strength

- Have a **unique password** for every account.
- Passwords should be at least 12-14 characters in length
- Avoid using:
  - Common names, such as the names of your family members, pets, movie characters, or car models.
  - Words that can be found in any dictionary, foreign language included.
  - Curse words
  - Common keyboard combinations such as adjacent letters and sequential numbers.

Two-Factor Authentication



Requires two pieces of information to log into an account:

- One may be something you know, like a password.
- The other may be something you have, like a code that’s sent to your phone.

Protect Your Most Important Accounts:

- With two-factor authentication, your accounts are much more likely to be kept secure.
- Most financial institutions now offer two-factor authentication.
  - Examples: E*Trade, Fidelity, Bank of America.
- Many popular sites also offer it.
  - Examples: Gmail, Yahoo! Mail, LinkedIn, Twitter, PayPal, Dropbox, Facebook, and Apple iCloud.

Social Media

Protect Your Identity:

- Know your social media contacts (including LinkedIn contacts).
- Set your security settings to the level of your comfort.
- Don’t post on social media:
  - Vacation or personal plans
  - Your full birthdate
  - Information on your children
  - Information on new purchases, such as jewelry, cars, or electronics

Public Wi-Fi

How to use Public Wi-Fi safely:

- **Consider the public Wi-Fi network as untrustworthy.**
  - Don’t conduct sensitive business (such as online banking or stock trades) over public Wi-Fi.
  - Don’t enter your login credentials to anything over Public Wi-Fi.
- If you receive a security warning when logged on to a public Wi-Fi network, log off immediately.
  - It’s okay for a security warning to display BEFORE login.
  - It’s NOT okay if a security warning displays AFTER login.
- **Verify the Wi-Fi network name with a trusted person before logging on.**
  - Hackers sometimes set up rogue networks with names that look legitimate.
- **Never install software or patch your applications on public Wi-Fi.**

Key Takeaways

Cyber attacks are ever-present and always changing

- Establish accountability and ownership for Information Security within your court.
- Ensure basic information security policies and protections are in place
  - Anti-virus, backups, system patching, strong passwords, etc.
- Prepare a cyber incident response plan
- Participate in testing your incident response plans
- Ensure your Technology Managers are proactively establishing a relationship with law enforcement partners

Qualcomm

Thank you!

Follow us on:

For more information, visit us at:

www.qualcomm.com & www.qualcomm.com/blog