Security Awareness

Introduction

- This is a guide to provide general information for individual, candidates, and organizations to help protect themselves against cyber security threats and attacks. It contains information on how to identify threats, general tips & advice, and ways to report an incident, if you believe you were a victim of a compromise (Fig 1.0 and 1.2 – right column).
- Please note Santa Clara County and the Registrar of Voters are not responsible for protecting individuals, candidates or campaigns against cyber security threats or attacks. This guide is also not a substitute for legal advice.
- While the information in this guide may be helpful to you, it is not a guarantee of security, even if these tips are followed.

Social Engineering Threats

Types of Social Engineering Threats

- Email Phishing: Attackers send well-crafted emails to convince users to click on a link, download an attachment, or redirect to a fake website in order to compromise a user's information.
- Fake Websites: An attacker sends an email to a recipient to click on a link and be redirected to a website to coerce the victim to give up sensitive information.
- Impersonation/Spoofing: A victim is deceived by an imitation of a reputable company, or through a phone call pretending to be a legitimate user such as a technical support staff. The example below (Fig 1.1) looks legitimate and encourages the user the click on the "check activity" box, which would send the user to a malicious website and steal their username and password, if entered on the website. It is always a best practice to go directly to the website by typing in the website's address yourself and not click on any links, if you wanted to verify an alert like below. Attackers can also mask/impersonate the "From:" field in an email also known as "Spoofing".

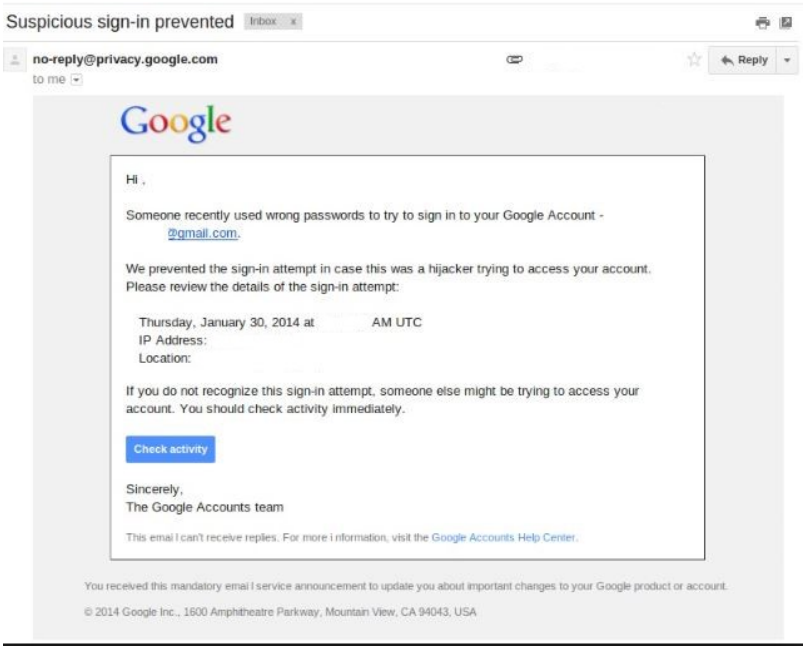

Fig 1.1 For additional information from Google regarding "Suspicious sign in prevented" emails, see *https://support.google.com/accounts/answer/6063333?hl=en*

Reporting

Fig 1.0

- Investigation Internet Crime Complaint Center (IC3) – www.ic3.gov
- Identity Fraud and Consumer Fraud - https://www.treasury.gov/services/report-fwa/Pages/id_theft.aspx
- U.S. Computer Emergency Readiness Team (US-CERT) - https://www.us-cert.gov/report-phishing

CISO

Malware Threats

Types of Malware Threats

- Ransomware: An attacker will encrypt the user's data and will extort the user to release the files.
- Keyloggers / Man-in-the-middle: A hardware/software that can capture a user's interaction with a system.
- Crypto-mining: An attacker will utilize a user's machine in order to conduct crypto-mining activities.

Preventive Measures

- Look out for generic salutations, grammar mistakes, and spelling errors scattered throughout the email.
- Provide security awareness training to all personnel.
- Limit or refrain from the publishing of sensitive, personal, organizational, or corporate information on the internet.
- Do not authorize a financial transaction or provide sensitive information via email.
- Only allow tech support that you recognize, if you do not know who they are, question them and make sure they are an approved employee.

General Tips & Advice

Practice good online safety habits with these tips and advice.

Keep a Clean Machine

- Keep software current: Ensure installed software receives the latest updates. This includes web browsers, anti-virus software, and operating system updates. These updates often contain security patches to protect against known vulnerabilities and threats.
- Automate software updates: Enable automatic updates. Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- Protect all devices that connect to the Internet: Computers, smartphones, TV's, gaming systems and other web-enabled devices (also known as Internet of Things or IOT) also need protection from viruses and require updates.
- Plug & Scan: USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information

- Lock down your login: Protect your online accounts by enabling multifactor authentication. This enables users to provide a password/pin in addition to biometrics (fingerprint or iris scan), security keys or a unique one-time code through an app on your mobile device.
- Make your password a sentence (passphrase): Make your password long, strong and complex. That means at least twelve characters, mixed with uppercase and lowercase letters, numbers, and symbols. Avoid common words, phrases or information in your passwords.
- Unique account, unique password: At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords and are not duplicated.
- Keep it safe: Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer. You can alternatively use a service like a password manager to keep track of your passwords.

Resources

Fig 1.2

- Defense Homeland Security - https://www.dhs.gov/sites/default/files/publications/Phishing%20508%20compliant%20508%20compliant.pdf
- OnGuardOnline - https://www.consumer.ftc.gov/features/feature-0038-onguardonline
- IRS - https://www.irs.gov/privacy-disclosure/report-phishing
- Scams and Identity Theft - https://www.consumer.gov/section/scams-and-identity-theft

Connect With Caution

- When in doubt, throw it out: Links in emails, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it. Some cybercriminals are able to compromise accounts of people you know and use the information stored in their inboxes to craft seemingly legitimate looking emails like the one below (Fig 1.3). Always be cautions and if it doesn't appear to be something you need to follow up with the individual, but still have doubts, use an alternate and known form of communication like a voice call.

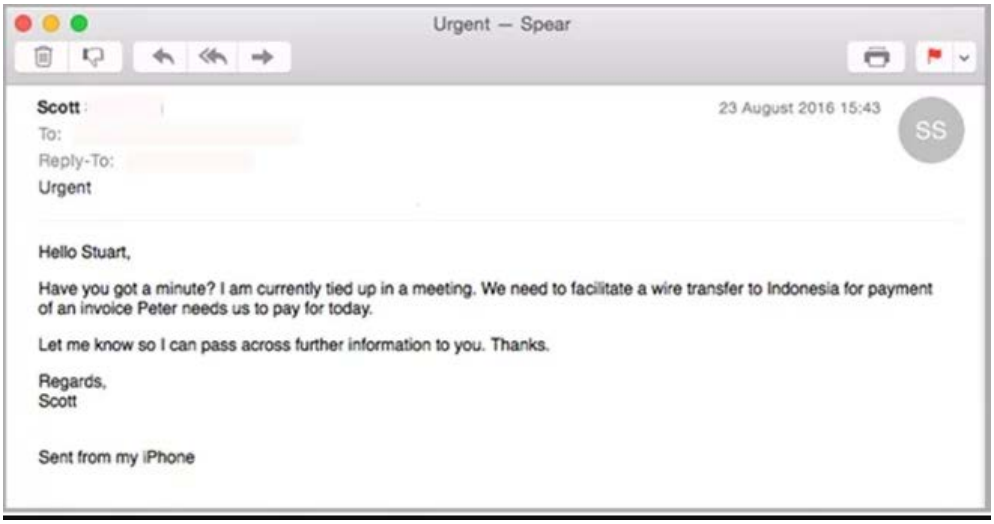

Fig 1.3

- Public Wi-Fi: Limit the type of business you conduct utilizing public Wi-Fi. Public Wi-Fi should not be used for conducting sensitive business.
- Protect your $$: When banking and shopping, check to be sure the site is security enabled. Look for web addresses with https:// which means the site takes extra measures to help secure your information. Http:// is not encrypted and thus has the potential to be viewed by an attacker.

Be Web Wise

- Think before you act: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true or ask for personal information.
- Back it up: Protect your valuable digital information by making an electronic copy and storing it safely.

Own Your Online Presence

- Personal information is like money. Value it. Protect it.: Information about you, such as your purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps and websites.
- Be aware of what's being shared: Set the privacy and security settings on web services and devices to your comfort level for information sharing.
- Share with care: Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it could be used now and in the future.
- Verify and protect your social media accounts: If using a social media account go through the "verification" process these services have. This will limit the risk of someone impersonating you. Also use strong passwords and Multi-Factor Authentication for these accounts as well. For example, in Fig 1.4 Twitter uses a "Blue verified badge" to let users know the Twitter account has been verified and it is the true entity posting information or "tweeting".

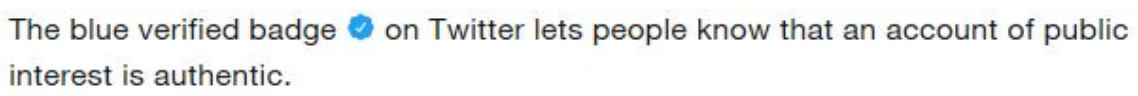

Fig 1.4 *(https://help.twitter.com/en/managing-your-account/twitter-verified-accounts)*