Powered by LAIKA

Security Awareness & Incident Response Training

Agenda

01

Security Threats

02

Information Security Best Practices

03

Incident Response

01

Security Threats

The Importance of Security Awareness

Security is everyone's responsibility.

The internet allows an attacker to work from anywhere on the planet. It is important for all of us to understand today's ever-growing online threats and take the necessary precautions to prevent a serious security issue.

- Risks caused by poor security knowledge and practice:
    - Identity Theft
    - Monetary Theft
    - Legal Ramifications (for yourself and your organization)
    - Sanctions or termination if policies are not followed
- According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:
    - Web Browsers
    - IM Clients
    - Web Applications
    - Excessive User Rights

Viruses

What are viruses? How do we avoid them?

- A virus attaches itself to a program, file, or disk.
- When the program is executed, the virus activates and replicates itself.
- The virus may be benign or malignant but executes its payload at some point (often upon contact).
- Viruses can cause computer crashes and loss of data.
- In order to recover or prevent virus attacks:
    - Avoid potentially unreliable websites/emails.
    - System Restore.
    - Re-install operating system.
    - Use and maintain anti-virus software.

Social Engineering

Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Phishing

Counterfeit Emails

A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.

Pharming

Counterfeit Web Pages

A link provided in an e-mail leads to a counterfeit webpage which collects important information and submits it to the owner.

The counterfeit web page looks like the real thing and extracts account information

Example: A social engineer sends an email that appears to come from a fellow employee asking the recipient to download an attachment or click on link.

Other Kinds

Pretext Phone Calls

Example: A social engineer calls and pretends to be a fellow employee or trusted outside authority (such as law enforcement, vendor, or an auditor)

Physical Social Engineering

Example: Piggybacking/Tailgating is where someone asks, “Can you hold the door for me? I don’t have my access card on me.”

Other Threats

What other threats should we be looking out for?

Worms

Independent programs that replicate automatically and send themselves to other computers by first taking control of certain software programs on your PC, such as email. Upon arrival, the worm may be activated to replicate.

Logic Bombs

Malware logic that executes upon certain conditions and destroys data. The program is often used for otherwise legitimate reasons. Examples include: Software which malfunctions if maintenance fee is not paid; Employee places logic bomb inside database to destroy data when he/she is terminated.

Trojan Horse

Masquerades as a benign program while quietly destroying data or damaging your system. It can be used to set up a backdoor in a computer system so that the intruder can gain access later. Example: A game that contains hidden code and sits on your computer gathering personal information without your knowledge.

Other Threats

What other threats should we be looking out for?

Botnet

A number of compromised computers, called zombies, used to create and send spam or viruses or flood a network with messages as a denial of service attack.

Man in the Middle Attack

An attacker pretends to be your final destination on the network. When a person tries to connect to a specific destination, an attacker can mislead him to a different service and pretend to be that network access point or server.

Rootkit

Upon penetrating a computer, a hacker may install a collection of programs, called a rootkit.

This may enable:

- Easy access for the hacker (and others) into the enterprise
- Keystroke logger

A rootkit also eliminates evidence of a break-in and modifies the operating system.

Identifying Security Compromises

Generally Suspicious Symptoms:

- Antivirus software detects a problem.
- Disk space disappears unexpectedly.
- Pop-ups suddenly appear, sometimes selling security software.
- Files or transactions appear that should not be there.
- The computer slows down to a crawl.
- Unusual messages, sounds, or displays on your monitor.
- Stolen laptop: 1 stolen every 53 seconds; 97% never recovered.
- The mouse pointer moves by itself.
- The computer spontaneously shuts down or reboots.
- Often unrecognized or ignored problems.

Malware/Spyware Symptoms:

- Changes to your browser homepage/start page.
- Ending up on a strange site when conducting a search.
- System-based firewall is turned off automatically.
- Lots of network activity while not particularly active.
- Excessive pop-up windows.
- New icons, programs, favorites which you did not add.
- Frequent firewall alerts about unknown programs when trying to access the Internet.
- Poor system performance.

02

Information Security Best Practices

Best Practices to Avoid These Threats

Defense in Depth uses multiple layers of defense to address technical, personnel and operational issues.

Defense in Depth Layers

- Data
- Application
- Host
- Internal Network
- Perimeter
- Physical
- Policies, Procedures, Awareness

Attack

- Hardware Broadband Router / Firewall
- OS / Software Firewall
- Antivirus / Antimalware
- Security Patches
- Vista UAC

Using Strong Passwords

What makes a good password? How do you create one? What are good password practices?

Lengthy

At least 8 characters or more

Complex

Mix uppercase, lowercase, numbers and symbols

Secret

Do not share with others or write them down

- **Do not use common or predictable passwords**
  - Examples of bad passwords: your own birthday, people's names, your phone number
- **Do:**
  - Use word combinations or full sentence phrases rather than single words
  - Incorporate acronyms or non-English language words
  - Substitute letters with numbers or symbols (e.g. p@ssw0rd$)

Safety Precautions

All employees should take the following precautions:

Trust, but verify.

It's each employees' responsibility to know who is requesting information from, from highly sensitive and confidential customer information to their own personal information. Social engineering - tactics used to gain access and steal valuable assets - is on the rise, so all employees must be watchful and mindful at all times.

Enable Anti-virus and Anti-Spyware Software.

- Anti-virus software detects certain types of malware and can destroy it before any damage is done.
- Install and maintain anti-virus and anti-spyware software.
- Be sure to keep anti-virus software updated.
- Many free and commercial options exist.

Enable Host-Based Firewalls.

- A firewall acts as a barrier between your computer/private network and the internet. Hackers may use the internet to find, use, and install applications on your computer. A firewall prevents many hacker connections to your computer.
- Firewalls filter network packets that enter or leave your computer

Safety Precautions

All employees should take the following precautions:

Protect your Operating System.

- Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
- The Windows Update feature built into Windows can be set up to automatically download and install updates.
- Avoid logging in as administrator
- Apple provides regular updates to its operating system and software applications.
- Apply Apple updates using the App Store application.

Practice Safe Web Browsing.

- Before logging into or entering sensitive information into a website, look for the security padlock symbol in the URL bar.
- Double clicking the icon will display the certificate information for the page you are viewing to guarantee that it is a safe, secure website
- The “https” is another indication that the page you are viewing is secure
- Pay attention to the web address - if it has changed or doesn’t seem right, it may be a fraudulent site
- Clear out browser sessions, temp files, cookies, history, saved passwords, etc. periodically, ensuring no pre-populated usernames and passwords exist especially on non-company owned desktops, laptops, and workstations.

Safety Precautions

All employees should take the following precautions:

Avoid Social Engineering.

- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their validity.
- Only visit and/or download software from web pages you trust.

Safely Navigate Popups.

- Pop-up blockers do not always block ALL pop-ups so always close a pop-up window using the 'X' in the upper corner.
- Never click "yes," "accept" or even "cancel."
- In order to close Scareware Popups, hold the **Alt+F4** key

Be Mindful About Emailing and Social Media.

- Don't use your personal email account for work purposes.
- Use secure email encryption whenever sending any restricted or sensitive information.
- Think before you post. Ask yourself, "*Does the posting or uploading of my personal social media resources disclose any "sensitive information" related to my company or does it in any way impact the safety and security of my organization?*"

Safety Precautions

All employees should take the following precautions:

Be Careful on Wireless Access Points.

- Wireless connectivity must be turned off when not in use.
- Only trusted Wi-Fi “hotspots” can be connected to.
- Wireless access points should not be used for conducting business activities, unless with an approved VPN and secure, remote access software on your laptop.

Protect Wireless Handheld Devices.

- Protect your devices with a password/PIN (6 digit recommended minimum)
- Use device encryption, remote wipe, GPS location, physical security
- Do not download apps from unknown sources
- Read what others are saying about the app in the reviews
- Avoid using public Wi-Fi hotspots, especially when accessing any password-protected sites or where you will enter any personal or confidential information
- When disposing any wireless handheld devices, ensure that all sensitive and confidential data has been removed, such as with a secure wipe program

Safety Precautions

All employees should take the following precautions:

Keep Up With Software Updates.

- Update all Internet browsers.
- Update all Operating Systems.
- Update Portable Document Format (PDF) / Adobe
- Keep a list handy of all the applications on your computer, making sure to perform security updates regularly.

Protect Your Laptop.

- Full-disk encryption must reside on all laptops ensuring the safety and security of data.
- Do not download or install into any drives or ports additional software that has not been approved as it may contain malicious files, could consume additional resources, or is simply not professional for work environments.
- Do not put any sensitive and confidential information on removable storage devices, USB ports, such as thumb drives or external hard drives.
- Do not transmit any sensitive or confidential information over instant messaging channels.
- If your laptop gets stolen, report the theft to local authorities along with informing management and the IT department immediately.

Physical Security Precautions

All employees should take the following precautions:

Be Mindful of General Physical Security In The Office.

- Question all strangers. Alert security guard and/or management to suspicious individuals.
- Be sure authorized visitors/contractors have properly checked in.
- Make sure individuals use their own key fobs/card keys when entering secure areas.

Follow the Clean Desk Policy.

- Always lock your computer screen whenever leaving your computer unattended.
- Configure your computer to automatically lock or engage password protected screensaver after an unattended duration of 15 minutes.
- Secure sensitive paper documents and turn work papers face down when leaving work areas unattended and at the end of the day.
- No documents containing confidential or sensitive information be left in the printer/copier area overnight.
- Use secure shred bins for disposing of sensitive paper documents and electronic media.

Incident Identification

Determining the Scope

Theft, damage, or unauthorized access
e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/ unauthorized physical entry

Fraud
Inaccurate information within databases, logs, files or paper records

Abnormal system behavior
e.g., unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals

Security event notifications
e.g., file integrity alerts, intrusion detection alarms, and physical security alarms

Critical customer complaints
e.g., Incorrect information showing on their account, any accusations of wrongdoing on behalf of the company

Internal operational incidents
e.g., no access to the building , e-mail issues

Process for an Incident

Determining the Scope

01 Identification

- Monitoring - Message to slack channel, or email notification
- Client complaints - email notification
- Direct Communication from Partners/Vendors - email notification

02 Initial Investigation

- Determine whether isolated incident
- Look for factors that could explain abnormal behavior
- Estimate potential impact

03 Reporting

- Email the IRT team

04 Initial Investigation

- Classification into Level 1 , 2 or 3
- Containment and Isolation
- Communication: Personalized message to top tier partners, Template response to other partners

05 Resolution

- Evidence Collection and Investigation

06 Communicating Resolution

- Personalized message to top tier partners, Template response to other partners

07 Review and Analysis

- Review all evidence collected
- Track investigation using TOOL

03

Incident Response

Process for an Incident

Classification and Containment

The IRT will first attempt to determine if the security incident justifies a formal incident response.

In cases where a security incident does not require an incident response the situation will be forwarded to the appropriate area of IT to ensure that all technology support services required are rendered.

The following descriptions should be used to determine what response the IRT will take:

- Level 3 – Limited impact or minor disruption to business operations. Isolated incident (Single Client).
- Level 2 – Important or severe impact. Important disruption of business operations.
- Level 1 – Negative impact to business reputation, negative client reaction, financial and liability impacts. A security incident impacting 25% of platform users must be set to Level 1.

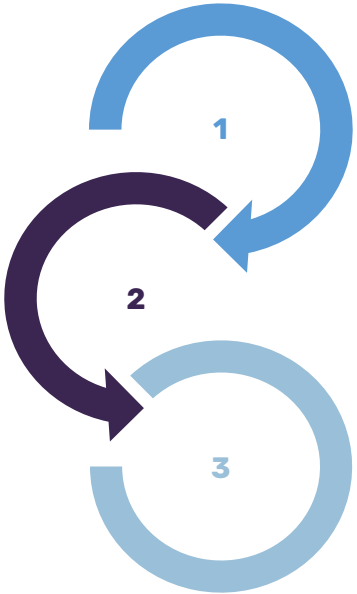
Process for an Incident

	Description	Incident Classification	Targeted Threshold
Resolution Time	Span of time of an incident, measured between opening the ticket and solving the ticket (status “Solved”)	Level 1/ High Level 2 / Medium Level 3	< 4 h < 24 h during office hours < 1 week during office hours (next release?)
Resolution Time	Span of time of an incident, measured between opening the ticket and assigning the ticket (status “In Progress”)	Level 1/ High Level 2 / Medium Level 3	< 30 Minutes < 1 h during office hours < 8 h during office hours

Process for an Incident

Analysis, Lessons Learned & Reporting

Not more than one week following the incident, members of the IRT and all affected parties will meet to review the following:



Results of the investigation conducted to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan.

Other security controls to determine their appropriateness for the current risks.

Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.