Cybersecurity Awareness

STATECIVILSERVICE
COMPREHENSIVE PUBLIC TRAINING PROGRAM

Phishing

Phishing defined - A high-tech scam that uses e-mail to deceive you into disclosing information.
The following are suspicious indicators related to phishing and spear phishing:

1. Uses e-mail
2. May include bad grammar, misspellings, and/or generic greetings
3. May include maliciously crafted attachments with varying file extension or links to a malicious website
4. May appear to be from a position of authority or legitimate company:
5. Your employer
6. Bank or credit card company
7. Online payment provider
8. Government organization

Spear Phishing - a type of targeted phishing that appears to be from a specific organization, such as your employer or bank

The following are suspicious indicators related to phishing and spear phishing:

1. Has a high level of targeting sophistication and appears to come from an associate, client, or acquaintance
2. May be contextually relevant to your job
3. May appear to originate from someone in your email address book
4. May contain graphics that make the email look legitimate

Effects of Phishing:

1. Deceives you into disclosing personal information
2. Allows adversary to gain access to your and/or your organization's information

The following countermeasures can be taken to guard against phishing and spear phishing:

1. Watch out for phishing and spear phishing
2. Delete suspicious e-mails
3. Contact your system security point of contact with any questions
4. Report any potential incidents
5. Look for digital signatures
6. Check for valid email addresses
7. Appears to direct you to a web site that looks real

Do Not:

1. Open suspicious e-mails
2. Click on suspicious links or attachments in e-mails
3. Do not click on ads or other questionable links on a web page
4. Call phone telephone numbers provided in suspicious e-mails
5. Disclose any information to an unknown source through any media – not email, text message, or phone calls

What to do if you're attacked:

1. Among other steps, if you fall for a phishing scheme, you should immediately change any compromised passwords and
2. disconnect from the network any computer or device that could be infected with malware because of the phishing attack. This will help limit the damage.

Weak & Default Passwords

Defined: Adversaries easily gain access to computer and network using legitimate login credentials

1. Create an easily exploitable system vulnerability
2. Is a vulnerability that is easily controllable by users

Effects include, but are not limited to, hackers:

1. Exploiting users' habit of repeating passwords across sites and systems
2. Cracking passwords to less secure sites
3. Accessing your and your organization's information

The following countermeasures can be taken to guard against password compromise, when creating a password:

1. Combine letters, numbers, special characters
2. Do not use personal information
3. Do not use common phrases or words
4. Vary the case in your passwords
5. Do not write down your password, memorize it
6. Change password according to your organization's policy
7. Enforce account lockout for end-user accounts after a set number of retry attempts
8. Do not save your passwords or login credentials in your browser
9. NEVER SHARE YOUR PASSWORD

Malicious Code

Malicious Code defined: Software that does damage and/or creates unwanted behaviors

Technique: Embeds malicious code into links which, once selected, download the malicious code to the user's computer and network. Malicious Code Includes:

1. Viruses
2. Trojan horses
3. Worms
4. Keyloggers
5. Spyware
6. Rootkits
7. Backdoors

The following are suspicious indicators related to malicious code; malicious code may be distributed via:

1. E-mail attachments
2. Websites
3. Removable media Is any type of storage device that can be added to and removed from a computer while the system is running. Malicious code can be stored in removable media devices. Once the device is activated, the code initiates and infiltrates the user's computer and any network connected to the computer

Effects include, but are not limited to:

1. Corrupt files and destroyed or modified information
2. Compromise and loss of information
3. Hacker access and sabotaged systems

The following countermeasures can be taken to guard against malicious code.
To guard against malicious code in email:

1. View e-mail messages in plain text
2. Do not view e-mail using the preview pane
3. Use caution when opening e-mail
4. Scan all attachments
5. Delete e-mail from senders you do not know
6. Turn off automatic downloading

To guard against malicious code in websites:

1. Block malicious links / IP addresses
2. Don’t download files
3. Block all unnecessary ports at the Firewall and Host
4. Disable unused protocols and services
5. Stay current with all operating system service packs and software patches

To guard against malicious code in removable media:

1. Follow your organization’s removable media policy
2. Do not use flash media unless operationally necessary and government owned
3. Do not use any personally owned/non-Government removable flash media on governments systems
4. Do not use Government removable flash media on personal systems
5. Encrypt all data stored on removable media
6. Encrypt in accordance with the data's classification or sensitivity level
7. Use only removable media approved by your organization

What to do if you are attacked:

Among other steps, if you fall for a phishing scheme, you should immediately change any compromised passwords

Ransomware

Ransomware Defined: Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return

Ransomware may be distributed via:

1. Email attachment
2. Clicking an ad
3. Following a link
4. Visiting a website that's embedded with malware

Effects: Most of the time, you don't know your computer has been infected. You usually discover it when you can no longer access your data, or you see computer messages letting you know about the attack and demanding ransom payments.

Countermeasures:

1. Keep operating systems, software, and applications current and up to date.
2. Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans.
3. Back up data regularly and double-check that those backups were completed.
4. Secure your backups. Make sure they are not connected to the computers and networks they are backing up.
5. Create a continuity plan in case your business or organization is the victim of a ransomware attack.

What to do if you're attacked:

1. Limit the damage - Immediately disconnect the infected computers or devices from your network. If your data has been stolen, take steps to protect your company and notify those who might be affected.
2. Contact the authorities - Report the attack right away to your local FBI office.
3. Keep your business running - Now's the time to implement that plan. Having data backed up will help.
4. Should I pay the ransom? - Law enforcement doesn't recommend that, but it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. However, paying the ransom may not guarantee you get your data back.

ADDITIONAL RESOURCES

To report a security threat or for more information on state policy and protocols, state employees may call the Office of Technology Services.

State employees may call:

Information Security Hotline Toll-free (844) 692-8019 or Local @ (225) 342-9288

State employees may email:
Information Security Team at InfoSecTeam@la.gov
Chief Information Security Officer at CISO@la.gov

For more information on this topic, CISA, the Cybersecurity and Infrastructure Security Agency, is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

Click on the link for CISA's *STOP. THINK. CONNECT. ™ Toolkit* provides resources for all segments of the community: https://www.cisa.gov/publication/stop-think-connect-toolkit

STATECIVILSERVICE
COMPREHENSIVE PUBLIC TRAINING PROGRAM