Cyber Space, the New Frontier:

Now, more than ever, people are sharing sensitive personal information about themselves online. Technology allows us to connect to each other around the world no matter our location, bank and shop online, and even control our televisions, homes, and cars from our smartphones. With this added convenience comes an increased risk of identity theft and Internet scams. Every time we connect to the Internet – at home, at school, at work, or on our mobile devices – we make decisions that affect our cybersecurity.

Did You Know?

½	Roughly half of American adults (110 million) had their personal information exposed by cybercriminals in 2015 alone.
65%	Two-thirds of Americans (65 percent) who use the Internet received at least one online scam offer during 2013.
34%	Identity theft has been at the top of the Federal Trade Commission's Top Consumer Complaints list for 15 years in a row.

Common Internet Scams:

To help protect yourself against online threats, here is a list of common Internet frauds from the Federal Trade Commission.

Identity theft is the illegal use of someone else's personal information in order to obtain money or credit. How will you know if you've been a victim of identity theft? You might get bills for products or services you did not purchase. Your bank account might have withdrawals you didn't expect. You may see unauthorized charges on your credit cards. You may even see new accounts opened in your name that you did not authorize. You may fail to receive regular bills or mail. You may be unexpectedly denied for a credit application (when you believe you should qualify).

Imposter scams happen when you receive an email or call seemingly from a government official, family member, or friend requesting that you wire them money to pay taxes or fees, or to help someone you care about.

"You've Won" scams occur when you get an email telling you that you have won a prize, lottery, or sweepstakes. Though the person seems excited for you to collect your winnings, they then tell you there is a fee or tax to pay for the prize and request your credit card or bank account information.

Healthcare scams happen when you receive a call, email, or letter that promises big savings on health insurance but claims that you need to provide your Medicare or health insurance information, Social Security number, or financial information to take advantage of the deal.

What Can You Do?

Keep all machines clean: Keep the software on all Internet-connected devices up to date. All critical software, including computer and mobile operating systems, security software and other frequently used programs and apps, should be running the most current versions.

Secure your accounts: Use passwords that are at least eight characters long and a mix of letters, numbers, and special characters. Do not share any of your usernames or passwords with anyone. When available, turn on stronger authentication for an added layer of security, beyond the password.

Get two steps ahead: Turn on two-step authentication – also known as two-step verification or multi-factor authentication – on accounts where available. Two-factor authentication can use anything from a text message to your phone to a token to a biometric like your fingerprint to provide enhanced account security.

Back it up: Protect your valuable work, music, photos and other digital information by regularly making an electronic copy and storing it safely.

When in doubt, throw it out: Links in email, 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.

Plug & scan: USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

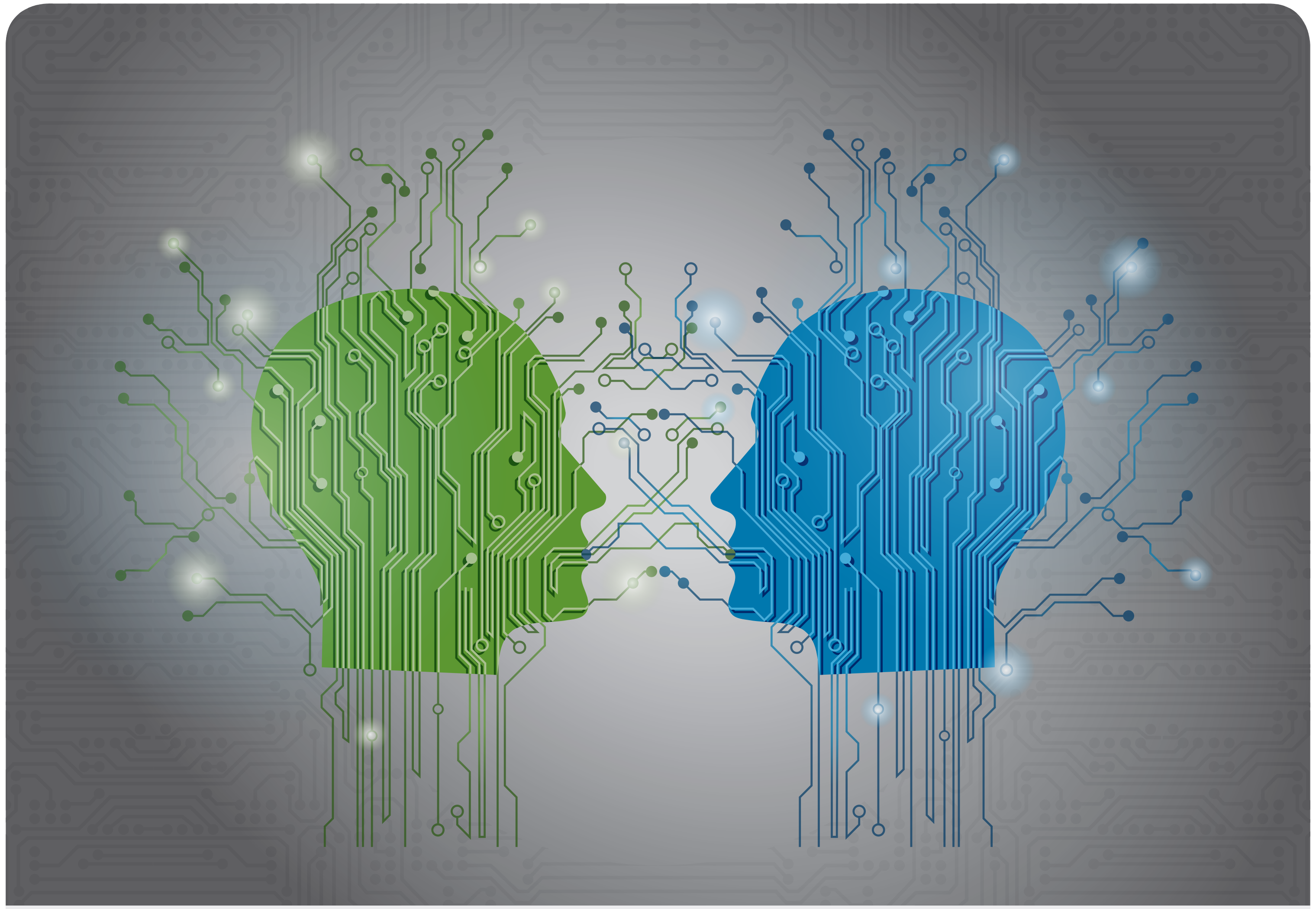
Report anything suspicious: If you experience any unusual problems with your computer or device, report it to your IT Department.

Guard your devices: In order to prevent theft and unauthorized access, never leave your laptop or mobile device unattended in a public place and lock your devices when they are not in use.

Good Information:

Department of Homeland Security	Cybersecurity: https://www.dhs.gov/topic/cybersecurity
Department of Homeland Security	Stop.Think.Connect: https://www.dhs.gov/stopthinkconnect
Lock Down Your Login	https://www.lockdownyourlogin.com/
Verizon Data Breaches Investigations Report (2016)	www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

U.S. DEPARTMENT OF HOMELAND SECURITY



Blue Hat Cyber Tabletop Exercise

Cyber Desktop Reference

May 23, 2019

Avoid Computer Misuse:

- ✓ Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- ✓ Change your passwords regularly (every 45 to 90 days).
- ✗ Do NOT give any of your usernames, passwords, or other computer/ website access codes to anyone.
- ✗ Do NOT open emails, links, or attachments from strangers.
- ✗ Do NOT view or download pornography.
- ✗ Do NOT gamble on your work computer.
- ✗ Do NOT conduct private business/money making ventures on your work computer.
- ✗ Do NOT load or use personal/unauthorized software or services, e.g. DropBox.
- ✗ Do NOT make any unauthorized configuration changes.
- ✗ Do NOT connect unauthorized USB devices to any system, to include cell phones.
- ✗ Only check personal email if your organization allows it.
- ✗ Don't play online games unless allowed by your organization.

Public Wi-Fi:

Think before you connect. Before you connect to any public wireless hotspot – like in an airport, hotel, or café – be sure to confirm the name of the network and login procedures with appropriate staff to ensure that the network is legitimate. Cybercriminals can easily create a similarly named network hoping that users will overlook which network is the legitimate one. Additionally, most hotspots are not secure and do not encrypt the information you send over the Internet, to include usernames and passwords, leaving it vulnerable to cybercriminals.

Use your mobile network connection. Your own mobile network connection, also known as your wireless hotspot, is generally more secure than using a public wireless network. Use this feature if you have it included in your mobile plan.

Avoid conducting sensitive activities through public networks. Avoid online shopping, banking, and sensitive work that requires passwords or credit card information while using public Wi-Fi.

Keep software up to date. Install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent cybercriminals from being able to take advantage of known vulnerabilities.

Use strong passwords. Use different passwords for different accounts and devices. Do not choose options that allow your device to remember your passwords. Although it's convenient to store the password, that potentially allows cybercriminals into your accounts if your device is lost or stolen.

Social Engineering:

Social engineers use telephone surveys, e-mail messages, websites, text messages, automated phone calls, and in-person interviews. To protect against social engineering:

- Do not participate in telephone surveys
- Do not give out personal information
- Do not give out computer or network information
- Do not follow instructions from unverified personnel
- Document interaction: verify the identity of individuals, write down phone number, and take detailed notes.
- Contact your security POC or help desk
- Report cultivation contacts by foreign nationals

Malware:

Malware, short for "malicious software," includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.

Adware	a type of software that downloads or displays unwanted ads when a user is online or redirects search requests to certain advertising websites.
Botnets	networks of computers infected by malware and controlled remotely by cybercriminals, usually for financial gain or to launch attacks on websites or networks. Many botnets are designed to harvest data, such as passwords, Social Security numbers, credit card numbers, and other personal information.
Ransomware	a type of malware that infects a computer and restricts access to it until a ransom is paid by the user to unlock it. Even when a victim pays the ransom amount, the stolen files could remain locked or be deleted by the cybercriminal.
Rootkit	a type of malware that opens a permanent "back door" into a computer system. Once installed, rootkits allow additional viruses to infect a computer as vulnerabilities are further exposed and compromised.
Spyware	a type of malware that quietly gathers a user's sensitive information (including browsing and computing habits) and reports it to unauthorized third parties.
Trojan	a type of malware that disguises itself as a normal file to trick a user into downloading it in order to gain unauthorized access to a computer.
Virus	a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files entirely.
Worm	a type of malware that replicates itself over and over within a computer.

Denial-of-Service:

Denial-of-Service (DoS) attacks refer to the use of specific tools by adversaries to cause networks and/or computers to cease operating effectively or to erase critical programs running on the system. Currently, Distributed DoS (DDoS) attacks are becoming prominent where a team of adversaries located in various geographical locations launch simultaneous attacks on a victim host. It is generally difficult to trace the source of DDoS attacks as intruders could launch the attack through multiple different gateways before reaching the victim host. In a DoS attack, DNS, web, and mail servers are the most likely targets. Some examples of DoS attacks are:

- Email related DoS (e.g., mail SPAM, mail bombs);
- Service related DoS (e.g., Slammer Worm, Chargen DoS), and
- Network jamming DoS (e.g., SYN flood DoS, 'Ping of Death' DoS, Smurf DoS).

Bots and Botnets:

What are Bots and Botnets?

There's no question that the internet is awesome; it makes our lives easier and connects us to the rest of the world. Unfortunately, there are bad guys out there who harness that convenience to do harm. One of the common types of cybercrime infects connected devices with specific types of malware, turning them into what are known as bots.

Once a device becomes a bot, it is usually part of a botnet – a larger network of other infected devices that are all controlled remotely by hackers. Cybercriminals use bots for financial gain or to steal, send spam to infect more devices or attack websites. A botnet can have anywhere from a few hundred to many thousand devices at its disposal.

Phishing:

Phishing attacks use email or malicious websites to infect your device with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their device with viruses or malware, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information like account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access their accounts.

Phishing Examples

The following messages, from the Federal Trade Commission's OnGuardOnline, are examples of what attackers may email or text when phishing for sensitive information:

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."	"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."	"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit www.irs.gov/uac/report-phishing.

Insider Threat:

We often think of cyber threats as coming from an anonymous criminal, hundreds of miles away behind a computer screen. However, current and former employees who have intimate and valuable knowledge about a company are also capable of committing a cybercrime. An insider threat occurs when a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data, intentionally misuses that access in a manner to commit a cybercrime.

Did You Know?

28%	electric crime events were known to be caused by insider threats.
46%	the most costly cybercrime events were a result of an insider threat.
34%	insider threat cases were targeted towards collecting personally identifiable information (PII).

Behavioral Indicators

A good way to prevent an insider threat is to train your employees to recognize some common behavioral indicators among their colleagues. US-CERT has identified the following behavioral indicators of malicious threat activity:

- Remotely accesses the network while on vacation, when sick, or at odd times during the day.
- Works odd hours without authorization.
- Unnecessarily copies material, especially if it is proprietary or classified.
- Expresses interest in matters outside the scope of their duties.
- Shows signs of drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health, or hostile behavior.