Cyber Attacks Training

What are the dangers of a cyber attack?

There are a number of different ways that hackers can attack their targets.

Malware	
Viruses and Worms	Viruses and worms are self-replicating programs that spread copies of themselves within and between computers. Viruses often hide alongside a non-malicious program downloaded from the internet. Worms operate as standalone programs that become active once the program is run for the first time. Both of these types of malware will actively try to use your computer and internet connection to infect other computers by first copying itself and infecting other programs and files on your computer.
Trojan Horses	Like a worm, a Trojan horse is a type of malware that pretends to be a desirable program. Once downloaded and activated, this malware is able to perform a range of attacks on the host computer, including sending all information typed into the keyboard back to the author of the malware. Unlike viruses and worms, Trojan horses do not copy themselves to infect other parts of a computer.
Ransomware	Ransomware is a type of malware that, once installed, stops the user from accessing certain parts of their computer and demands that a ransom be paid in order for access to be restored. While some ransomware can be reversed by an IT professional, more advanced malware may encrypt the data on the computer, making it much harder – or impossible – to reverse without providing payment.

What are the different methods of cyber attack?

Now that you know a few of the dangers that hackers pose, here is a list of the methods hackers often use to spread those dangers:

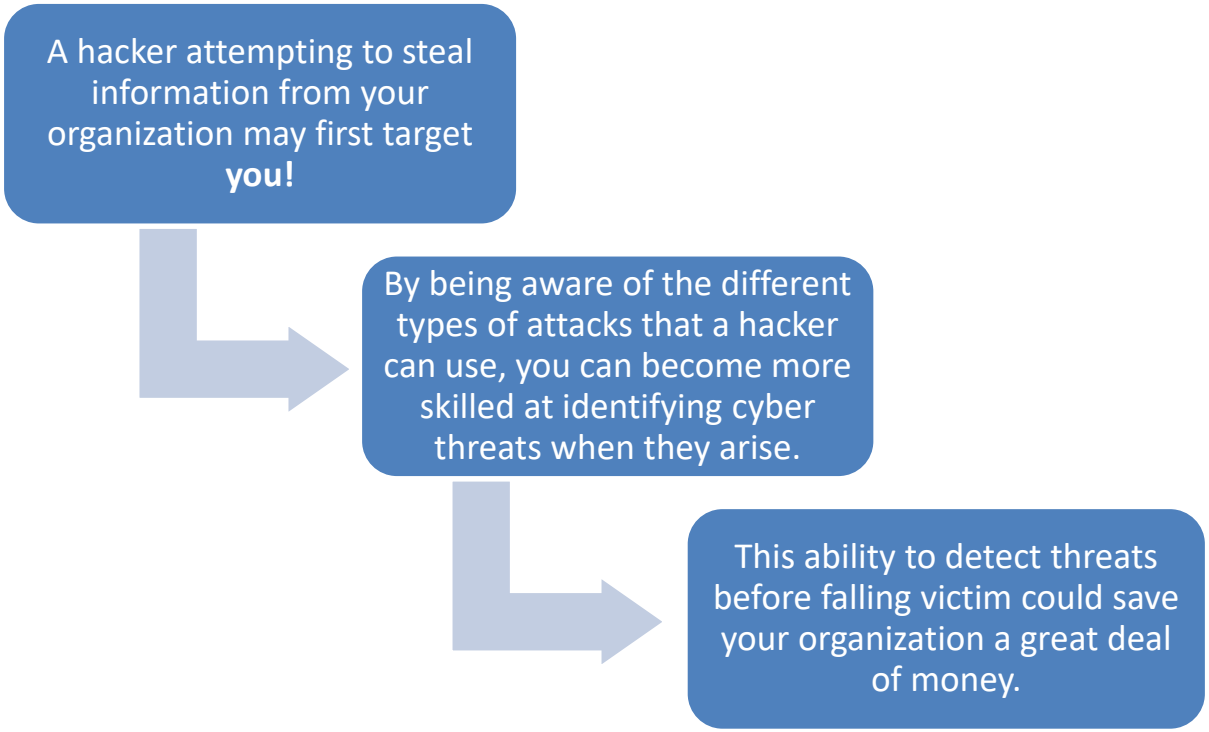
Social Engineering	
Phishing	Phishing is an attempt by a hacker to gain critical and/or personal information from a computer user by pretending to be a trustworthy source and asking for account information, banking information, money, etc. The most commonplace phishing occurs through email. Often phishing emails will contain spelling and grammar errors. This is done on purpose to ensure that the victims who fall for the first scam will continue to fall for subsequent requests for personal information or money.
Spear Phishing	While phishing emails are usually sent to large volumes of users, sometimes a hacker will have a very specific target in mind. When this occurs, phishing emails become personal and believable. These are referred to as spear phishing attempts. Even legitimate-looking emails that ask for personal information, money, etc. should be treated with extreme caution despite the apparent trusted source.
Physical	Not all social engineering attempts are done using technology. People can be tricked by a hacker even when they are away from their computer. Hackers posing as computer repair professionals, couriers, or company employees may try to gain access to an organization's critical information by physically entering the establishment.

What are the different methods of cyber attack? (continued)

Other	
Advanced Persistent Threats	An Advanced Persistent Threat is an attack on a network. Once the hacker gains access to the target network, they try and remain undetected for a long period of time. Rather than cause damage, these attacks are focused on listening to – and stealing – the information passed along this network.
Spam	Unsolicited messages received on the computer are called electronic spam. While these messages are often attempting to advertise a product, they may contain disguised links that send the user to fake websites that are pretending to be legitimate. Any information that is entered into this fake website, including payment information and account credentials, will be sent to the website's author without alerting the spammed user.
Wi-Fi Eavesdropping	Hackers are able to listen in on information that is passed over an unsecure public Wi-Fi network. This includes usernames, passwords, emails, banking information, etc. Encryption is used by some websites to prevent hackers from easily reading the information sent over the network. However, a hacker could still crack this encrypted information with the right tools and expertise.

Sources: TechTarget definition of "advanced persistent threat (APT)"
Wikipedia definition of "Email spam"

How Does It Affect You and Your Organization?



30% of data breaches globally are caused by employees that are unaware of the threats that exist on the internet today (Ponemon Institute, “2014 Cost of a Data Breach Study”).

Threat Identification

How can you tell if your computer has been compromised?

A Slow Computer

Sometimes, a slow computer means that your system has been infected. Malware tends to slow down your computer's operating system, making applications unusually slow.

A Crashing Computer

If you find that applications or your entire computer often crashes unexpectedly, it may be infected with malware.

Annoying Pop-ups

Getting unwanted pop-ups is a sign that your computer has been infected. Often the malware causing the pop-ups is doing further damage to your computer in the background.

Fake Email/Social Media Messages

If your friends/colleagues tell you that they have received messages from you that you didn't send, your computer is likely infected with malware and it is trying to infect other people.

Unexpected Software

If you notice software on your computer that was recently downloaded without your permission, it is likely a malicious program.

Disabled Antivirus Software

Certain types of malware will disable your antivirus software when your computer becomes infected.

Threat Identification

How can you tell if somebody is trying to phish you?

Too Good To Be True

Emails that promise free trips, prizes for contests you didn't enter, or money are most likely phishing emails. If you respond, you will probably be asked for personal information or an increase in the number of spam emails you receive. Report or ignore these emails and send them to your trash bin.

Personal Information Requests

Phishing emails may ask you for personal information, such as your email account credentials and bank account information. Unexpected requests for personal information are almost always a hoax. Often a hacker will disguise this request with an urgent matter – e.g. your email account has been deactivated. Please enter your email username and password to enable it again.

Bad Spellers

Emails from unfamiliar senders that are full of spelling and grammar mistakes should be treated with caution. Scammers are looking for gullible people; if a person is gullible enough to fall for an email with many language errors, they are more likely to divulge additional personal information or money.

An Unfamiliar Sender

When receiving an unexpected email, look at the email address of the sender. Unless you recognize the sender, treat the email with extreme caution.

False Identities

Viruses can be spread through social media websites. These viruses will send messages to an account's contacts asking them to click on a link. Just because a message comes from a friend does not mean that they sent it to you. If anything seems suspicious, ignore the message and alert the user.

Reporting and Contact Information

If you have any general questions:

- Bruin Support Services at 1.800.756.7920

Be Proactive

There are many activities that can help protect you and your device from the dangers hidden on the internet:

- ✓ Before downloading a program from the internet, make sure you trust the website, your firewall is currently active, and an up-to-date antivirus program is installed on your computer. These precautions will reduce the chance of your computer becoming infected by malware.
- ✓ To avoid falling victim to a ransomware attack, regularly back up your computer files. When/if a ransomware attack strikes, a copy of all your files will be safe on your backup device. Once the malware has been removed, the damaged files can be replaced with the backup versions.
- ✓ Watch for suspicious emails all the time. These could be emails asking for personal information or account credentials, emails with surprising spelling and grammar errors, emails with unknown senders, or emails with offers that seem too good to be true.
- ✓ Do not use public Wi-Fi networks for activities that involve entering personal information or account credentials. This information can be seen by a hacker currently listening to the Wi-Fi network.

A private, non-profit institution founded in 1966, Bellevue University is accredited by the Higher Learning Commission through the U.S. Department of Education. For general information, please call 1.800.756.7920.