VAStar Cyber Security

Cyber Security Fundamentals

Goals

- Learn to identify good and bad passwords and create strong passwords
- Learn about password managers and how to use them
- Learn about antivirus software and the malware that it protects against
- Learn about public records, online research, and social engineering
- Learn about classic cryptography methods and how they were used in the past

Passwords

Passwords are both the easiest gateway to data and the biggest deterrent. A strong password is unbreakable by the strongest computers for millions of years, but a weak password can be cracked almost instantly.

Creating a strong password is easier than many think. Although adding numbers and special characters do help make a password harder to guess, the most important factor is length. The longer the password, the harder it is to crack. Having different passwords for every system helps protect data when one password is compromised.

This comic explains this principle: https://xkcd.com/936/

Typically 12 characters in length will make a strong password. Using the site https://howsecureismypassword.net/ test some password combinations to see how hard they are to crack.

Good and Bad Passwords

Bad passwords are easy to spot. Some of the most used passwords are 'password', 'password1', and 'qwerty'. Continuing to add length will make a password stronger. An extremely strong password will also mix upper case letters, lower case letters, numbers, and special characters. This adds to the possible characters that make up the password, making it harder to crack.

Good Passwords	**Bad Passwords**
!hAmmer0Spaghetti)wow	123456
Interesting89pOrk$	Password
Butter is my favorite food!	qwerty
This is a strong password.	letmein

Password Managers

A password manager is an application which stores and protects a user's passwords to facilitate strong and varied password use. Research the following password managers and explain the pros and cons of each.

- LastPass
- DashLane
- 1Password
- KeePass

Antivirus Software

Antivirus software is used to keep computers safe from viruses, trojans, spyware, ransomware, and other malicious software. Many malicious programs are designed to be 'silent'. They don't alert the user to the fact that they are installed, and usually steal data or grant access to a malicious actor.

Antivirus software can help detect and remove these malicious programs, keeping computers and data safe from intrusion.

Firewalls

A firewall is a hardware or software network component that monitors and controls network traffic based on security rules. A firewall can detect and stop malicious network traffic before it is sent to the destination computer.

Firewalls are usually a network's first line of defense against a network-based attack by an outside actor. If the malicious actor is already inside the network, however, the firewall won't help deter them.

Public Records & Online Research

Sometimes hackers use computers to impersonate people or gain access to their information. One of the ways they do this is through online research. There is a surprising amount of information available online for hackers to find. Between social media and public records, hackers can have enough information to pretend to be their target. Pick a person and research online to try to find their:

- Date of Birth
- Social Media Accounts
- Address
- Court Records
- Birth Records
- Marriage Records
- Business Records
- Death records

Social engineering

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. Social engineering is one of the largest ways by which hackers gain access to secure systems. Imagine calling your cell phone company and pretending to be someone else in order to gain access to their account or wearing a high visibility vest and a radio to access a secure location. These are examples of social engineering.

Social Engineering Phone Call: https://www.youtube.com/watch?v=nknq9sUu8ko

Many large companies are working hard to develop software which is less prone to social engineering by requiring the user to enter information which only they should have access to in order to modify a record.

Classic Cryptography

Cryptography is the study of codes. Codes have been used for all of history to securely transport messages to their recipient without anyone else reading them. Wars have been won and lost all through history because of codes. Some of the most famous codes include the Caesar Cipher (which helped Julius Caesar encode military messages while dominating much of Europe) and the Enigma machine (used to protect both commercial and military messages by Nazi Germany during World War II).

Symbolic Encoding

Swapping letters or words for a symbol is one of the oldest methods of hiding information. Sometimes letters are swapped for well-known standards for the purpose of transmitting (Morse code/Telegraph, ASCII - Binary/Computers) while other times the encoding is designed to keep the message secret.

The most famous symbolic encoding method is named 'Mary, Queen of Scots'. Named after an actual queen, Mary wanted to assassinate Queen Elizabeth I and used messages encoded with symbols to communicate with her co-conspirators. Elizabeth's codebreaker broke the code and Mary was executed in 1587.

Try a modern version using emojis to send a message here: https://codemoji.org

Caesar Cipher

The Caesar Cipher (or shift cipher) is one of the best known forms of encryption. This signifies a change from encoding where a message was hidden with a set of substitutions for each letter to one where the only knowledge needed is a key to "unlock" the message. In the 1st century BCE, Julius Caesar used this cipher to encode military messages. In the 1980s, a special form of the Caesar Cipher called ROT13 was used by usenet newsgroups to hide lewd jokes.

The Caesar cipher works by taking a message and shifting its characters down by a specific amount known only by the sender and the recipient. For example, using a key of 23, "THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG" becomes "QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD".

Here is an example of the shifted alphabet:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Try developing a code with your peers and exchanging messages.

More classic cryptography

Research online the following ciphers and explain their pros, cons, and use.

- Substitution Cipher
- Vigenere Cipher
- One-Time Pad
- Hill Cipher
- Bacon's Cipher
- M-94 Cipher
- Four Square Cipher