6 types of cybersecurity attacks:

1. Malware

Malware-short for "malicious software"-is software specifically designed to gain unauthorized access to or damage a device, typically without the owner's knowledge (but not always). Common types of malware include:

Trojan horses: malware disguised as a legitimate program that provides a hacker backdoor access to your computer

Viruses: malware designed to change, corrupt, or destroy information that is then passed on to other systems, usually by otherwise benign means (like sending an email)

Spyware: malware that is used by hackers to spy on your computer or mobile phone activities

Worms: malware that can multiply and spread to other computers in the network

Most malware is unknowingly downloaded through this process:

- A hacker strategically places an infected link, file, or attachment in the path of a victim, usually through a phishing email or other social engineering tactic.
- The victim clicks on the malicious asset, triggering the malware to install onto their device.
- The hacker can use the malware to steal, compromise, and/or destroy data stored on the device.

Some cybercriminals will use USB sticks or flash drives to install malware onto a computer because it's harder for some cybersecurity systems to detect. To avoid this, never leave your computer or other device logged in and unattended, and never insert an unfamiliar storage device into your computer.

2. Ransomware

Ransomware is malware that can lock, encrypt, and destroy personal files once it gains access to your computer. Like the name suggests, hackers typically use ransomware to extort money from their victims with promises of restoring the encrypted data.

Ransomware is a growing concern for organizations and individuals. More than 2,000 devices were infected with ransomware in 2021 alone, and hackers reaped more than $6 million in average payouts from victims in the U.S.

3. Distributed denial-of-service (DDoS) attacks

Similar to ransomware, distributed denial-of-service (DDoS) attacks also compromise computer availability. DDoS attacks are used by cybercriminals attempting to flood or crash a website by triggering traffic from millions of botnets. Here's how it works:

- The hacker forms a "zombie network" of remotely controlled hacked computers called botnets.
- The hacker uses the zombie network to flood a targeted website or internet server with traffic, rendering it inoperable.
- Once the website or server crashes, both website administrators and online visitors won't be able to access it.

At a minimum, a DDoS attack will result in a temporary loss of service or website performance issues that could impact revenue for a business. However, DDoS attacks can also be used to hold a site hostage until a ransom is paid. Some hackers have even used DDoS attacks as a smoke screen for other malicious activities.

4. Phishing

Have you ever received a message from one of your Facebook friends asking you to check out a deal they received on an expensive purse or new pair of sneakers? Chances are their account was hacked and used in a phishing scam.

Phishing is a cybercrime scammers use to try to lure sensitive information or data from you by impersonating a trustworthy source, like a friend or your bank. Phishers can trick you by sending links asking for personal information like your credit card or Social Security number through:

- Text message
- Email
- Phone calls
- Social media direct messages

Some phishing schemes are obvious-common red flags include poor grammar and odd-looking URLs. However, scammers are developing more sophisticated tactics to lure you into sharing your information.

For example, in 2018 phishers targeted Netflix users through an email stating the popular streaming platform was "having some trouble" accessing the customer's billing information. The message asked users to click on a link to update their payment method. That link, of course, didn't take users to Netflix but instead to a fake website created by the hackers.

5. Advanced persistent threats

Advanced persistent threats (APTs) are a type of attack on integrity used to infiltrate a network undetected for an extended period of time, all the while stealing valuable data without actually harming the network. APTs have the ability to destroy and manipulate files stored on computers and devices, targeting data like:

- Legal contracts
- Patent information
- Medical records
- Blueprints
- Financial documents

While large organizations and government platforms are typically the targets of APTs, individual users can also fall prey to this type of cyberattack. Some of the consequences of an APT attack include:

- Theft of intellectual property
- Distribution of sensitive information
- Site takeovers
- Session hijacking
- Destruction of data

6. IoT-based attacks

From STEM toys to smart home technology, the popularity of Internet of Things (IoT) devices is on the rise. It's important to keep in mind that any device connected to the internet is prone to cyberattacks and should have cybersecurity measures in place to protect you and your personal information.

Cybercriminals take advantage of the security shortcomings characteristic of many IoT devices (IoT devices are particularly vulnerable to malware attacks and ransomware) to gain access to other devices on the network. Luckily, there are cybersecurity best practices to prevent these types of attacks.