

# CYBER ATTACK

## WHAT IT IS

Unlike physical threats that prompt immediate action, cyber threats and attacks are often difficult to identify or comprehend. Cybersecurity involves preventing, detecting, and responding to cyber incidents. Virtually all modern organizations – including governments, hospitals, corporations, banks, and utilities – rely on computer systems for their operations and data management, and are therefore vulnerable to cyber attacks.

The so-called "attack surface" that may be vulnerable to bad actors can include computer hardware, tablets, phones, and many other web-enabled devices and appliances in the so-called "internet of things." Among the dangers of cyber attacks are intruders erasing entire systems, holding data or operating systems for ransom, stealing confidential or personal information, breaking into systems and altering files, or using a computer or device to access contact lists and attack or infect others.

## KEY TERMS

- A **Cyber Attack** may originate from individuals, networking groups, terrorist groups, or countries, and may cause severe (and dangerous) problems for government, business, utilities, and the general public.
- **Hacking** is a direct attack against a system "through the wires" in which an attacker (be they live or an automated "bot") gains direct access to secured/restricted data or operations. Often the pathways that allow such hacks are opened via "phishing" or download scams.
- The **Internet of Things (IoT)** includes web-enabled devices and appliances including refrigerators, sound systems, clocks, thermostats, security systems, coffee makers, etc.
- **Phishing** consists of broadly disseminating email or text communications in the hope that a few recipients will click somewhere in the message (for example an attachment, a link, an "enable macros" button) that activates a virus or other malware. A targeted phishing campaign – for example, against a particular government or utility – is called spear-phishing.
- **Social Engineering** involves exploiting the vulnerabilities of a user, rather than their system, to circumvent IT security measures. Examples include phishing, email scams, and other cons. Users are often the most easily defeated element of IT security architecture.

## WHAT TO DO

### Before (Preparedness/ Mitigation)

- ❑ Keep your firewall turned on and updated.
- ❑ Install or update antivirus/ antispyware software.
- ❑ Use strong, unique passwords, and change them on a regular basis.
- ❑ Seek out and promptly install all updates to your operating system, firmware, software, and antivirus.
- ❑ Be careful what you download. Never click on an attachment, link, or macro in an unsolicited email or text.
- ❑ Turn off your computer when you are not using it.
- ❑ Always verify the source of emails, and if in doubt delete them.
- ❑ Be suspicious of emails from known contacts that seem "off" – misspellings, strange syntax or word usage, generic language, weird link URLs – many hacking campaigns will impersonate known emails.
- ❑ Screenshot suspicious content before deleting it, for analytics.
- ❑ Regularly back up all of your data to an external hard drive or the Cloud; enable the "Time Machine" feature if you use a Mac.

### During (Response)

- ❑ Disconnect an infected device from your network.
- ❑ If you are at work, inform your IT staff of any suspected or confirmed attacks on your devices, and provide a screenshot.
- ❑ If an incident incurs in loss of financial, personal, or medical information, file a police report.

### After (Recovery)

- ❑ Notify anyone that could be adversely affected, including your credit accounts, bank accounts, clients, employer, family, and friends. Change your accounts and all passwords.
- ❑ Run appropriate scans and utilities to remove any infections.
- ❑ Monitor your credit report, banking statements, investments, and credit card statements.
- ❑ Ensure your device is not infected, and wipe the hard-drive and reinstall all software if there is any doubt.