

# American College of Radiology

---

Language course: “We speak Cyber”

*Cybersecurity is a complex topic. We want to make it more accessible and easier to understand – friendly to the layperson.*

*If you are an expert, feel free to skip this part.*

*We call this an ABC of Cybersecurity.*




## How to use this document:


Like with any language course, the vocabulary of the different proficiency levels of “We speak Cyber” are built upon each other:

1. [Beginner](#)
2. [Elementary](#)
3. [Intermediate](#)
4. [Advanced](#)
5. [Fluent](#)

You can click on all vocabulary in the “[contents](#)” section and jump there directly.

Almost all vocabulary is explained via:

-  **Definition:** a theoretical definition of the concept
-  **Analogy:** a “translation” from the cyberworld into an easy-to-understand metaphor
-  **Example:** back to the world of cyber, a real-life example of the topic

Additionally, the sign “” lets you know that there is a link you can click to get to a further reference.

---

## CONTENTS

<b>Beginner .....</b>	<b>4</b>
Cybersecurity .....	4
Hardware.....	4
Memory stick .....	4
Server.....	4
Software .....	4
<b>Elementary .....</b>	<b>5</b>
Backup .....	5
Data privacy .....	5
Hacker.....	6
Networks .....	6
LAN /// Local area network.....	6
WAN /// Wide area network.....	6
WLAN /// Wireless local area network .....	7
Operating system .....	7
Plugin .....	7
Threat.....	7
Vulnerability.....	8
<b>Intermediate .....</b>	<b>8</b>
Cloud.....	8
Cloud service.....	8
Malware.....	8
Patching .....	9
Removable media .....	9
<b>Advanced.....</b>	<b>9</b>
Attack surface.....	9
Attack vector.....	9
Authenticity.....	10
DoS /// Denial of Service .....	10
Detection .....	10
Compromised system.....	10
Credentials .....	11
Cybersecurity goals.....	11
Confidentiality .....	11
Integrity.....	11

---

Availability.....	12
Encryption .....	12
Payload .....	12
Phishing .....	12
Ransomware .....	13
Remote access.....	13
Smishing .....	14
Social engineering.....	14
<b>Fluent.....</b>	<b>15</b>
Arbitrary code execution.....	15
Cryptocurrency .....	15
Cryptojacking.....	16
NAS /// Network attached storage.....	16
Recovery .....	17
RCE /// remote code execution.....	17
Virus protection .....	17
Zero-day.....	18

---


# BEGINNER


---

## Cybersecurity

---

 **Definition:** Cybersecurity protects a cyberspace from cyberthreats.


 **Analogy:** You can imagine the coined term "cyberspace" quite literally as a space in the real world, let's take the living room of your home, if you will. Cybersecurity is the protection of said room from (cyber) threats – i.e. hackers.


 **Example:** your LinkedIn password (your cybersecurity measure) protects your profile (your cyberspace) from unauthorized access and people posting untrue things in your name (the cyberthreat).


---

## Hardware

---

 **Definition:** the physical component(s) of a computer.


 **Analogy:** the muscles of your body parts like arms or legs – something you can touch and feel.


 **Example:** your computer mouse, the keyboard, the circuit board or fans.

---

## Memory stick

---

 **Definition:** electronic memory data storage devices used for storing data, typically in portable devices.


 **Analogy:** taking a cool drink out of your fridge at home, putting it into a portable cooler and bringing it to the picnic.


 **Example:** the SD card in your camera, the USB stick on your desk.


---

## Server

---

 **Definition:** basically a computer that does something for another computer.

 **Analogy:** you go to a restaurant and ask the literal server, a.k.a. waiter, to bring you a plate of food from the kitchen.


 **Example:** when you visit a web page, your phone (the client) is asking another computer (the server) for a page. The server builds it and sends it to you.

---

## Software

---

 **Definition:** the programming on your computer.

 **Analogy:** the thoughts and skills within your brain – you can't touch them but without them you are pretty much useless.

---

 **Example:** the operating system (Windows or Apple IOS) or the applications (Powerpoint or Siri) or the system settings (language set to Chinese).


---

# ELEMENTARY


---


## Backup

---

 **Definition:** a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event:

- verb form, referring to the process of doing so is *back up*
- noun and adjective form is *backup*.

 **Analogy:** You give your sister a copy of your house key so that if you ever lost your key, your sister can give you her copy to enter your house.

 **Example:** your iPhone automatically asks you if you want to have an “iCloud backup” stored on your Macbook, so if you lose your iPhone and buy a new one, you can simply plug it in and have your Macbook restore all of your settings on the new device.


---


## Data privacy

---

 **Definition:** the branch of data management that deals with handling personal data in compliance with data protection laws, regulations, and general privacy best practices.

Note: data privacy is *not* data security! Security can exist without privacy principles, but privacy needs security — in fact, there is no privacy without security.

 **Analogy:** like the rules at your home. If salt or pasta is out, write it on the grocery list. Take that list with you when you go shopping. Whoever cooks with the resource “salt” needs to make sure not to accidentally poison anyone. Everyone knows what to do with the resource.

 **Example:** Data privacy laws specify how data should be collected, stored, and shared with third parties. The most widely discussed data privacy laws include:

- **GDPR:** The European Union’s General Data Protection Regulation (GDPR) is the most comprehensive data privacy law in effect. It applies to European Union citizens and all companies that do business with them, including countries not based in Europe. GDPR gives individuals the right to determine what data organizations store, request that organizations delete their data, and receive notifications of data breaches. Noncompliance may result in hefty fines and legal action.
- **CCPA:** The California Consumer Privacy Act (CCPA) is a state-level regulation in the United States. It enables California residents to ask organizations what personal data exists about them, delete it on request, and find out what data has been given to third parties. These measures apply to consumer data gathered within the state.

---

## Hacker

---

🎓 **Definition:** someone who illegally tries to access another (person's) cyberspace. And these "threat actors" perpetuate cyberthreats.

💡 **Analogy:** a criminal breaking and entering your home.

🖥️ **Example:** Lisbeth Salander, Anonymous, Mr. Robot .... this is an ever more common theme in pop culture.

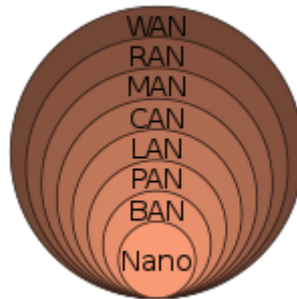
---

## Networks

---

There are multiple possible networks for computers to communicate with each other:

- The devices handling the network traffic get bigger and faster as the network size increases,
- but no fundamental difference from the technical viewpoint.
- There is also a difference in responsibility/ownership.



### *LAN /// Local area network*

🎓 **Definition:** a computer network that interconnects computers within a limited area. LANs are operated by a single entity for their own purposes, usually - you have a LAN at home, and a company's network at one site is also a LAN. So, the provider of a LAN has a direct relation to the customer using it - they are identical.

💡 **Analogy:** having a doorbell with an intercom system, so you can talk to the person outside.

🖥️ **Example:** a hospital network, where machines inside the hospital can talk to specific websites in the hospital but those sites can't be reached outside the hospital.

### *WAN /// Wide area network*


🎓 **Definition:** A collection of computers and network resources connected via a network over a geographic area. Bigger than a LAN, transporting data for customers without any local or city-wide focus, including the Internet as a whole. The providers of WAN have no additional relation to their customers, they just transport the data regardless of origin and target


💡 **Analogy:** using your cellphone to call your grandma 3 states away.

🖥️ **Example:** commonly connected either through the Internet or special arrangements made with phone companies or other service providers.

## WLAN /// Wireless local area network

 **Definition:** the *same* as LAN - but no wires.


 **Analogy:** your kids playing around and using walkie-talkies


 **Example:** commonly used in home environments to connect computing devices, wearables, smart appliances, etc.


---

## Operating system

---

 **Definition:** the giant underlying program that provides the bridge between hardware and software, for example Windows, Mac OS, or Linux.


 **Analogy:** we must go one step larger than your house – think of a frat house on a university campus, where people have to share fridges, bathrooms, there are common chore plans so everyone knows when to use and do what. There is a system that makes sure the frat house is operational.


 **Example:** The idea is that the developer of e.g. the Firefox browser doesn't need to write their program specifically to use the hardware on your computer: Firefox does not specifically use your keyboard or the mouse. The developer will write the application to work on Windows or on OS. Your operating system then figures out how to use the necessary hardware components (mouse, keyboard, screen) to give Firefox the tools to do what it's supposed to. An OS is also responsible for scheduling programs to run at the same time and make sure they fairly share system resources. You don't want to have to close your internet browser so you can open a word document.


---

## Plugin

---

 **Definition:** a way to extend a piece of software beyond it's original scope and standard functionality.


 **Analogy:** your dad fixing up the basement or garage to turn it into a home gym as needed. You can still park your car there and use it for whatever it was originally intended, but the scope has been upgraded.


 **Example:** on some websites sometimes cannot directly play videos – you need a plugin. Some laptops do not have a CD reader; you need to plug in an external CD drive.


---

## Threat

---

 **Definition:** an event or circumstance with the potential to harm your operations.


 **Analogy:** a robber watching you leave your key “hidden” underneath the doormat out front and stealing it.


 **Example:** a hacker sending you a phishing email and prompting you to enter your password and thereby stealing it.


---

## Vulnerability

---

 **Definition:** a weakness in a system that could be exploited or triggered by a threat.

 **Analogy:** leaving the key to your front door “hidden” underneath the doormat.

 **Example:** a user writing their password on a post-it and sticking it on the laptop screen.

---


# INTERMEDIATE


---

---

## Cloud


---

 **Definition:** the idea is to provide computational power and server space as a commodity like electricity.

 **Analogy:** To get electricity to your house, there are two main methods:

- a) Generate it yourself (generator, solar panels) or
- b) Connect your house to the electric company


Option a) is complex, so someone had the idea to generate a bunch of electricity in one place (electric companies) and sell it to people as they needed it. This way, you paid for as much as you used, even if you have a “spike” in usage, e.g. during the holiday time because of Christmas decorations.

 **Example:** when you use Apple cloud, Apple handles the complexity of storage, servicing servers and the application management. You pay a fee for their service that you use, you do not need the local storage on your iPhone in front of you – your pictures are saved on an Apple server somewhere else.


---

## Cloud service

---

 **Definition:** this used to simply be called “hosting” and today means any feature provided by a cloud provider. Common cloud services are storage (like Apple does for your photos), virtual servers or AI management.



 **Analogy:** paying for an Uber to the airport instead of driving yourself using your car.

 **Example:** if a million people decide they want to play Farmville at the same time, servers are automatically fired up to serve them. It'd be far too expensive to buy all the computers needed for these spikes and own and service them.

---

## Malware

---

 **Definition:** malicious software, refers to any intrusive software *intentionally* designed by cybercriminals (also known as  [hackers](#)) to steal data and damage or destroy computers and computer systems.

---



💡 **Analogy:** the “tools” a robber would use, e.g. a spyglass to check if you are home, a “fake call” to determine if you are *really* not at home and a hammer to crash the window pane and access your home.

📁 **Example:** computer viruses, computer worms, 👉 [ransomware](#), keyloggers, Trojan horses, spyware.

---

## Patching

---

📖 **Definition:** a patch is a set of changes to a computer program or its supporting data to update, fix, or improve it.

💡 **Analogy:** exchanging the lock on your front door after reading that the manufacturer had produced it with a flaw – many more keys than just yours were able to unlock it accidentally. You then exchange the lock, to be on the safe side.

📁 **Example:** when your browser tells you to updates automatically.

---

## Removable media

---

📖 **Definition:** expendable storage designed to be inserted and removed from a system.

💡 **Analogy:** see also 👉 [memory stick](#).

📁 **Example:** optical discs (e.g. Blu-rays, DVDs, CDs) or memory cards (e.g. Memory stick)

---

# ADVANCED

---

## Attack surface

---

Read 👉 [attack vector](#) first.

📖 **Definition:** the sum of the different points (for 👉 [attack vectors](#)) where an unauthorized user (the 👉 [attacker](#)) can try to enter data to or extract data from an environment.

💡 **Analogy:** if the lock on your front door does not work, and you also don't have a watch dog plus the security camera is currently broken – each of these problems is a vulnerability which makes the attack surface on your house rather large.

📁 **Example:** improperly discarded 👉 [hardware](#) or passwords written on paper.

---


## Attack vector

---

📖 **Definition:** a specific path, method, or scenario that can be exploited to break into an IT system, thus compromising its security.

💡 **Analogy:** whether a robber break into your house by smashing in the cellar window or by guessing the right pin to your electronic door opening system.

---


 **Example:** hackers using phishing emails versus unpatched software or simply stealing a company laptop.


---

## Authenticity

---

 **Definition:** refers to the veracity of the claim of origin or authorship of the information.


 **Analogy:** a hand written document you could compare the handwriting characteristics of the signature to a sample of others whose signatures have already been verified.


 **Example:** a digital signature can be used to verify the authorship of a digital document.


---

## DoS /// Denial of Service

---

 **Definition:** an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.


 **Analogy:** imagine the driveway to your house. you can usually drive in and out of it fine when theres no traffic. If there are a few hundred cars of traffic on your street, it is going to be hard and time consuming to get out of your driveway.


 **Example:** a Denial of Service can be caused by perfectly legitimate use as well, and in this case, the “legitimate” example is easier to understand than an attack: during Black Friday sales, when thousands of users are clamoring for a bargain, this might often cause a denial of service and the website is not reachable anymore.


---

## Detection

---

 **Definition:** the practice of analyzing the entirety of a security ecosystem to identify any malicious activity that could compromise the network.


 **Analogy:** installing a security camera on your garage and front door to make sure you are aware of trespassers. Or: buying a watch dog for your front yard and teaching it to bark when it sees an intruder.


 **Example:** the anti-spam software you installed in your browser lets you know, how many pop-ups it has disabled.


---

## Compromised system

---

 **Definition:** a system is compromised if there has been a breach in the confidentiality, integrity or availability of its infrastructure or components in any form.

 **Analogy:** you see the downstairs window is broken, so you are sure that in some form, the security of your home is compromised – even if you don’t know what has happened yet or to what extent.

 **Example:** There are many! Gaining unauthorized access to a computer by impersonating a legitimate user or by conducting a brute-force attack would constitute a compromise, exploiting

a loophole in a computer's configuration would also constitute a compromise. Depending on the circumstances, a computer infected with a virus, worm, trojan or other malicious software may be considered compromised as well.


Symptoms of a compromised computer include, but are not limited to, the following:


- Frequent pop-up windows, especially the ones that encourage you to visit unusual sites, or download antivirus or other software
- Changes to your home page
- Mass emails being sent from your email account
- Frequent crashes or unusually slow computer performance
- Unknown programs that startup when you start your computer
- Programs automatically connecting to the Internet
- Unusual activities like password changes


---

## Credentials

---

 **Definition:** evidence attesting to one's claim of identity or assertion of an attribute and usually are intended to be used more than once.


 **Analogy:** your government issues IDs such as a passport or a driver's license.

 **Example:** login credentials authenticate a user when logging into an online account over the Internet. At the very least, the credentials are username and password; however, a physical or human biometric element (e.g. touch ID) may also be required or additional security via two-factor authentication.


---


## Cybersecurity goals


---

The bigger picture is that cybersecurity teams try to accomplish 3 things  for the cyberworld they protect, these are the three classic security attributes of the so-called [C.I.A. triad](#)


### Confidentiality


 **Definition:** cybersecurity wants information to be accessible only to authorized individuals.


 **Analogy:** only you and the people you give a key can access your home and your belongings  
- no criminal can get in and take your stuff.

 **Example:** only clinical employees have access to a patient's medical records.


### Integrity


 **Definition:** cybersecurity wants the information to be accurate, i.e., uncorrupted, and unaltered.


 **Analogy:** your teenagers pile of laundry is inexplicably growing larger every week, because their peers pass around clothes and exchange jerseys after soccer practice. And you simply don't know which items of clothing you own anymore, so you just wash it all and might buy them a new shirt because the one you've just washed looks a tad small. In short: you waste resources (time and money as well as mental capacities in making the wrong decisions).

 **Example:** hackers will try to put false information into a system or change information already in the system, which results in no one being able to trust information in the system anymore.

### Availability

 **Definition:** cybersecurity wants the information and system to be accessible and usable when required.


 **Analogy:** if criminals can't steal from you or make you doubt yourself, they will take your house hostage and use it as they see fit. They may change the locks on your house, preventing you from accessing it.


 **Example:** if they can't inflict the other two attack types, hackers will try to make sure no one can use the system.


---

## Encryption

---

 **Definition:** is defined as the conversion of something to code or symbols so that its contents cannot be understood if intercepted. Encryption attempts to make information unreadable by anyone who is not explicitly authorized to view that data. People or devices can be authorized to access encrypted data in many ways, but typically this access is granted via passwords or decryption keys.


 **Analogy:** you remember in childhood you had a “secret code or language” with your best buddy, so no one could understand you? Basically that.

 **Example:** if you visit a website that is encrypted, these website URLs will begin with <https://www.acr.org> and most browsers will display a lock in the address bar to indicate the session is encrypted. While being transmitted, the data is encrypted and then decrypted once it reaches your browser. Information transferred between you and the secured website is only visible to you and the destination to which you are connected.


---

## Payload

---

 **Definition:** the part of transmitted data that is the actual intended message. Headers and metadata are sent only to enable payload delivery.


 **Analogy:** your neighbor’s invitation to their BBQ is sent in an envelope, but the real message is the invite letter itself – not the envelope used for delivery.


 **Example:** in the context of a computer virus or worm, the payload is the portion of the malware which performs malicious action.


---

## Phishing

---

 **Definition:** sending deceptive messages to end users to entice them to reveal confidential information, such as passwords.

 **Analogy:** your doorbell rings, you answer the door and your “new neighbor” is outside asking you whether they can come in or not – you are suspicious, because you’re not really aware anyone new has moved to the neighborhood, therefore you don’t grant access.

 **Example:** one of the most popular phishing templates is the fake invoice technique. Like many phishing attacks, this scam relies on fear and urgency, pressuring an end user to submit a payment for goods or services they’ve never even ordered or received:

---

**From:** xero [mailto: ]  
**Sent:** Tuesday, 20 June 2017 12:09 p.m.  
**To:** [redacted]  
**Subject:** Your xero invoice available now.

Hi ,

Thanks for working with us. Your bill for \$373.75 was due on 28 Aug 2016.

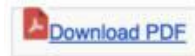
If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

To view your bill visit <https://fn.xero.com/5LQDhRwfvoQfeDtLDMqkk1JWSqC4CmJl4VVJRsGN>.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Thanks



NJW Limited







---

## Ransomware

---

 **Definition:** a type of  [malware](#) that threatens to either publish the victim's data or perpetually block the victim's access to the system unless a ransom is paid.


 **Analogy:** your dog got stolen from your front yard and a note is in your mailbox – you will only get her back if you pay a ransom.


 **Example:** Ransomware is a form of malware that  [encrypts](#) a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the  [decryption key](#).

---

## Remote access

---

 **Definition:** connection to a data-processing system from a remote location, for example, through a virtual private network. This means you are connecting two computers. One is your remote computer that you have sitting in front of you, and you use a program (e.g. TeamViewer) to “dial into” another target computer.

 **Analogy:** you can't talk to your spouse yourself because they are away for the weekend, therefore you facetime. You are not physically there, but the iPhone (the “target”) transports your face and voice remotely to your spouse.

**Example:** if you have an issue with radiology equipment in your hospital, you can usually call the IT service of your supplier and they can support you remotely by dialing into your system and fixing the issue for you – without needing to fly to you, the target location.

---

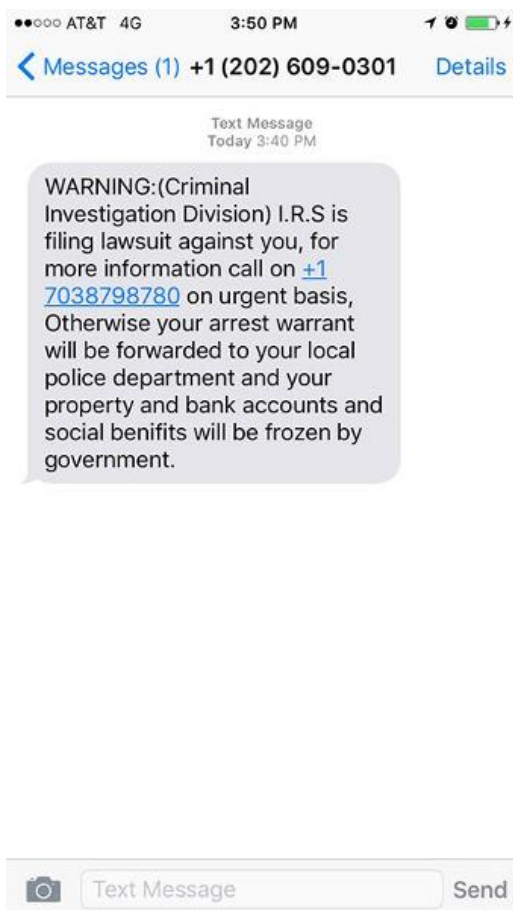
## Smishing

---

**Definition:** a form of [phishing](#) in which an attacker uses a compelling *text message* to trick targeted recipients into clicking a link and sending the attacker private information or downloading malicious programs to a smartphone.

**Analogy:** children sometimes do “phone pranks” with friends where they (try to) trick people on the phone into thinking they are someone else or into running outside so they can watch and have a laugh.

**Example:**



---

## Social engineering

---

**Definition:** the psychological manipulation of people into performing actions or divulging confidential information - a manipulation technique that exploits human error.

---

💡 **Analogy:** when you use "social skills" (convincing, lying) to make people do something, e.g. by telling the secretary it is really very urgent for you to get an appointment or using your title to create pressure.

📖 **Example:** pretending to be from the IRS and demanding someone's bank account information.

---

## FLUENT

---

### Arbitrary code execution

📖 **Definition:** an attacker's ability to run any commands or code of the attacker's choice on a target machine or in a target process. This is done locally on the target system!

💡 **Analogy:** when getting a new motorcycle license, often younger people are only allowed to or supposed to drive throttled engines. Now if they go to their buddy who can dethrottle it so they have full range of power.

📖 **Example:** in reality, this is more often something users do *themselves* on locked down devices. For instance, the Nintendo Switch is a locked down device, it only allows people to play games Nintendo has approved to be published for the switch and they put in a lot of effort to make sure that no games or software can be played without Nintendo's approval. Now you can "hack" into your own Nintendo Switch to play more games than the "allowed" ones. In contrast, 👉 [Remote Code Execution](#) is generally used in a malicious context.

---

### Cryptocurrency

📖 **Definition:** Cryptocurrencies are a digital form of currency, that is not reliant on any central authority, such as a government or bank, to uphold or maintain it. Individual coin ownership records are stored in a 👉 [digital ledger](#), which is a computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership.

This is a **big deal** because throughout the history of "normal" currencies, counterfeiting has been a big issue – and when it comes to digital anything, it is very simple to make a copy of things. This ease of duplicating information has made it hard to make a currency, because the second the currency becomes popular, it will become easier to fake it than earn it. However, cryptocurrencies have created a way for people to convert their efforts into a digital token system, and those tokens have proven to be secure from duplication – the above-mentioned *ledger*.



💡 **Analogy:** Before currencies existed, you had individuals trading and bartering their services with other individuals. Let's say you have Al, Bob, Crystal, and Dave living together in a society. Al is a dentist, Bob is a woodworker, Crystal owns the land rich in timber, and Dave is a blacksmith, they trade directly e.g., Bob makes a chair and gets a dental exam from Al.



Currencies are a sort of "economic buffer." Currency allows people to convert their efforts into something that maintains its value and can be converted back into goods or other services at a later point in time. Say, for example, Al wants a chair from Bob, but Bob doesn't want his teeth looked at. Bob makes the chair, delivers it, and, in return, Al gives Bob a piece of paper that says, "This paper is good for 1 dental exam." That piece of paper now has a value associated with it, because that paper represents a dental exam from Al. Now: Bob values Crystal's timber more than he values a dental exam. So Bob agrees to give Crystal his piece of paper from Al in exchange for timber.

Now it would have been easy for Bob to counterfeit the piece of paper, for this reason, currencies have largely relied on stuff from the real world that is scarce or finite, e.g. gold. Fast forwarded a bit more, and we have largely gone off the gold standard. This means that currency is, itself, the resource. The government "mints" currency, which means the government creates scarcity in the currency, as well as protects against people counterfeiting it. This trust and value gives the currency its value.


Cryptocurrencies are digital equivalents of currencies, and mimic natural limitations via very sophisticated programming: Bob as a bitcoin, the public ledger says he mined it himself and he can pay for the dental exam with said bitcoin, the same as he could with a real 20\$ bill.


 **Example:** Bitcoin, first released as open-source software in 2009, is the first decentralized cryptocurrency. Since the release of bitcoin,  [many other cryptocurrencies](#) have been created.

---

## Cryptojacking

---

 **Definition:** a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency.


 **Analogy:** your neighbor plugging his electric lawn mower into your garage socket and "stealing" your electricity.


---

## NAS /// Network attached storage

---

 **Definition:** a hard drive that is attached to a network and it's accessible over the network.

 **Analogy:** like a photo album in your living room that everyone is free to access and look at. The photos are in the album for all to view, not "private" in your bedroom.

 **Example:** often used by people in a shared home setting to share files between their computers, phones, backup solutions, smart TVs, etc. Think of it as a very large hard drive containing music movies TV shows that you can access with a variety of different devices. In a sense, it enables you to "build your own Netflix" with the use of appropriate software.

Obviously if you have movies and TV shows stored on your computer, you can watch them on your computer. What the NAS does is allow smart TVs, tablets, and phones to access that information without the need for the computer. In fact, you can even access your NAS when you are away from home.

The NAS can be viewed as "a small custom built computer that lets multiple devices access content".

---



---

## Recovery

---

📖 **Definition:** focuses explicitly on disasters resulting from cyber threats, such as 👉 [DDoS](#) attacks or data breaches. Your recovery plan will detail the steps your organization needs to take to stop losses, end the threat, and move on without jeopardizing the future of the business.

*Disaster recovery: the use of alternative network circuits to re-establish communications channels in the event that the primary channels are disconnected or malfunctioning.*

💡 **Analogy:** if there is an electric outage, you would have flashlights or candles in your house to use until the electricity comes back on.

📖 **Example:** a recovery plan contains different action items, these steps can include but are not limited to the following:

1. Identify what is lost and the extent of the damage.
2. Notify affected individuals and the respective offices.
3. Replace old systems and technologies with robust systems and apply security patches where necessary.
4. Validate the integrity of your remaining data, deploy backups where available.
5. Know your company's compliance obligations, both in terms of what obligations your organisation may have to others and what obligations others may owe to it.
6. Determine how the security breach may have affected stored sensitive data and what privacy legislations may be in breach and plan remediation.
7. Educate employees about keeping strong passwords and passphrases, identifying and avoiding cyber threats, what to do during an attack, and how to report a cyber threat.
8. Purchase cyber insurance for your facility.

---

## RCE /// remote code execution

---

📖 **Definition:** the ability to trigger 👉 [arbitrary code execution](#) over a network (especially via a wide-area network such as the Internet). The term is generally used in a malicious context, it means a hacker has gained control of your computer to some extent and can execute “code” (i.e. run a program) from anywhere.

💡 **Analogy:** if you have a smart home and are coming back from your vacation, you can already tell the furnace to heat up – remotely from your car.

📖 **Example:** like in pop culture, a hacker remotely being able to turn on the webcam on your laptop.

---

## Virus protection

---

📖 **Definition:** a kind of 👉 [software](#) used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

💡 **Analogy:** like when you go to the doctor for regular check-ups and have them scan your moles to make sure there is no malicious tissue.

📖 **Example:** there are many different styles of viruses and attacks, a lot of antivirus software deployed rely on a currently known threats or vulnerabilities. It is hard to defend against an unknown 👉 [vector of attack](#), but some basic attacks/detections are as follows:

1. **Size:** An easy way to detect if a file has been altered is the size of the file. Some viruses like to tack on their malicious code at the end of the file, and that is a dead giveaway when an antivirus scanner scans it. It compares the before and after sizes, and if there has been no modification by the user, it suspects some malicious activity.
2. **Deeper threats:** plug an 👉 [external device](#) into your computer, there is a code' that runs to setup the connections from your computer to the external device. Some viruses try to exploit this when the connection is being established, and could execute 👉 [arbitrary code](#) – a virus scan program can detect this.

---

## Zero-day

---

📖 **Definition:** if a flaw isn't fixed by 👉 [updates](#), then it is a known exploit. However, a zero-day attack takes place when hackers exploit a flaw that no one else knows about - so *before* developers have a chance to address it. It is called a Zero-Day because the good guys have had "zero days" to set up mitigation measures.

Zero-day is sometimes written as 0-day. The words vulnerability, exploit, and attack are typically used alongside zero-day, and it's helpful to understand the difference:

- A zero-day *vulnerability* is a software vulnerability discovered by attackers before the vendor has become aware of it. Because the vendors are unaware, no patch exists for zero-day vulnerabilities, making attacks likely to succeed.
- A zero-day *exploit* is the method hackers use to attack systems with a previously unidentified vulnerability.
- A zero-day *attack* is the use of a zero-day exploit to cause damage to or steal data from a system affected by a vulnerability.

💡 **Analogy:** you go on vacation and think you have taken care of everything but while you are gone, a robber finds out you've left the garage door unlocked. You have zero days to fix it and the attacker can exploit the flaw.

📖 **Example:** the [recently discovered Log4J vulnerability](#) (zero-day vulnerability) was discovered by hackers and zero-day exploited (Log4Shell), see here an "[explained like I'm 5](#)" article on this explicit example.