Cybersecurity Badges

Glossary for Juniors

Acknowledge means to make known that you received or accepted something. For example, "I acknowledge that you gave me a cookie." Or "I acknowledge that you won the game."

Binary is a way of representing information using only two options. For example, turn off or on are a set of binary options.

Binary code is the language a computer uses to process information. When you go online or play a video game, there is binary code behind the scenes that spells out what the computer should do.

Cipher is a way to change a message to hide its meaning, such as using special numbers, letters, and symbols in a code.

The **cloud** is a network of large computers or servers where internet information and data is stored.

A **code** is a system of symbols, such as letters or numbers, which are used to create a secret message. Code is also the language computers use. When you write code on a computer, you give it commands to tell it what to do.

A **computer virus** is a type of malware that spreads a bad code that can destroy data on your computer. Computer viruses make your computer's files "sick," the same way a virus makes a person sick.

Connect means to join two or more objects together. For example, a railroad's train tracks are connected to each other. A hallway connects two rooms.

Cybersecurity refers to how people keep their digital information from being stolen and protect it against cyber attacks.

Data is information that is made on or stored by a computer. Your music downloads and emails are examples of your data.

A **device** is a piece of equipment—such as a cell phone, computer, or tablet—that either works like a computer or is attached to a computer.

An **email** is a message that is sent electronically from one device to another.

A **hacker** is a person who uses computer skills to solve a problem with technology. There are different kinds of hackers. White hat hackers are people who tinker with computer systems to protect them. Companies sometimes hire white hat hackers to look for mistakes in their security systems so they can be fixed. Black hat hackers are criminals who break into someone else's computer or a company's computer system and cause harm. White hat hackers can help keep black hat hackers from committing crimes.

(continued)

An **identity** is made up of all the information that makes you different from other people. Your name and birthday are part of your identity.

Identity theft is a crime where someone steals your private information, such as your name, address, or Social Security number (a one of a kind number the government gives each person), and uses it to commit fraud. Identity thieves may use your information to open bank accounts, apply for credit cards, or make purchases—all in your name.

An **imposter** is someone who pretends to be someone else.

The **internet** is a group of computers and servers that are connected to each other.

Log in or **log on** is what you do when you want to get on to a website that is password protected. You can log in or log on to computers, mobile phones, tablets, or other digital devices. You might need a username and password, which is your log in information.

Malware is software that can cause damage to your computer. The damage can include stealing your information, slowing down your computer, or even causing it to stop working completely. Viruses, worms, and spyware are some examples of malware.

A **message** is a communication in writing, talking, or by signals. In the computer world, you send messages through emails, chats, and by texting.

A **network** is a system of computers and other devices (such as printers) that are connected to each other.

A **password** is usually a series of letters, numbers, and symbols used to get on to a computer or website. A computer password is private and used by one person only.

A **protocol** is a system of rules that explains the correct steps to follow.

Phishing is when a cyber criminal tries to get your private information by sending you a fake message.

Private information are facts about you that you don't want everyone to know. For example, your home address or the name of your school is private information. You don't want to share that with strangers.

Ransom is money paid in order to free something from a criminal. For example, this could be money you pay a criminal to get back something they stole from you.

A **scam** is a dishonest way someone can get something from another person, such as private information or money.

A **server** is a computer that serves other computers that are connected to it. Servers answer requests, deliver web pages, and more. When you go to a website, you are connecting to the site's server.

(continued)

A **Social Security number** is a one of a kind number the United States government gives each person. Your social security number may be the most important one you will ever have. You will need one when you go to college, when you get a new job, and when you open a bank account. Your social security number is part of your identity and part of your private information.

Synchronize is when two actions are arranged to happen at the same time and speed. For example, when you and your friend do a dance in exactly the same way, you are synchronized.

Trust means to believe in something or someone. When you trust someone, such as your family, you know they are trustworthy and it's OK to share something private.

A software **update** fixes parts of the software that aren't working. Updates also fix weaknesses in the software's security so your device can stay protected from hackers and malware. All digital devices—including smartphones, laptops, tablets, smartwatches—need to be updated regularly.

A **username** is a name, word, or characters you type so you can use a computer, cell phone, tablet, or website. Usernames are also called user IDs. Usually you need to type your username and a password.