Cybersecurity basics for beginners: 2024 guide by norton

What is cybersecurity?
Cybersecurity refers to every aspect of protecting critical systems, devices, and sensitive data against cyberattacks. From individual users to large multimillion-dollar corporations, having effective cybersecurity practices in place is essential for safeguarding your sensitive personal and financial information online.

Cybersecurity terms to know
Here are a few common cybersecurity terms you'll come across — or may have already:

- **Network:** interconnected digital devices that can exchange information and resources with one another
- **Internet protocol (IP) address:** a unique numerical identifier assigned to every device or network with internet access
- **Virtual private network (VPN):** an encrypted internet connection from a device to a network
- **Hacker (black hat):** a malicious person who attempts to gain unauthorized access to a network with the intent to cause damage or theft
- **Hacker (white hat):** A person who attempts to gain unauthorized access to a network in order to identify and patch vulnerabilities in a security system
- **Firewall:** a network security feature designed to monitor incoming and outgoing network traffic in order to block unauthorized access
- **Domain Name System (DNS):** a directory of domain names that align with IP addresses so users can search via URLs
- **Encryption:** the process of scrambling readable text so that it can only be read by the person who has the encryption key
- **Authentication:** the process of verifying a user's identity in order for them to access a system and/or data, like two-factor authentication
- **Data breach:** often the result of a successful cyberattack that results in the exposure of personal data, like credit card or Social Security numbers.

Cybersecurity fundamentals:
To grasp the fundamentals of cybersecurity, we'll need to break down the CIA triad. The CIA triad refers to the three principles of cybersecurity: confidentiality, integrity, and availability.
The CIA triad model serves as the basis for the development of most cybersecurity systems. Ideally, you'll want to meet all three standards to help protect yourself against cyberattacks.

Confidentiality
Confidentiality refers to the measures you take to ensure your data is kept secret or private. This includes personal information like:

- Credit card information
- Social Security numbers
- Physical addresses

- Medical records
- Account login information

Cybercriminals may make a direct attempt to steal this information with techniques like man-un-the-middle (MITM) or phishing. Once the hackers have access to this data, they can take control of your accounts or sell the information on the black market.

However, human error and insufficient security protocols may also play a role in a confidentiality breach. For example, using weak passwords or leaving your computer unattended could put your sensitive data at risk.

Integrity

Integrity in cybersecurity means ensuring your data remains trustworthy, accurate, and safeguarded against unauthorized modification or destruction.

This can be done by:

- Using end-to-end encryption to protect sensitive data while in transit and at rest
- Setting access controls so only authorized personnel can access specific information
- Ensuring no one user is given enough access to be able to misuse a system on their own
- Backing up data

Maintaining integrity is especially important for sites or users that provide important information to the public or organizations that handle sensitive information. For example, when a hacker published a fake news story under the guise of the Associated Press in 2013, the Dow Jones Index slumped by 150 points when the public believed the White House and President Obama had been attacked.

Integrity attacks can have huge implications for individuals as well. For instance, if a cybercriminal is able to access a bank database, they could manipulate the automated routing process to steal money and account information.

Availability

Even with effective confidentiality and integrity practices in place, a cybersecurity system is useless if it's not available to the user(s) it's intended to serve. Availability ensures that systems, networks, and applications are functioning so authorized users can access data when they need to.

Here's an example of availability most of us can relate to. When mandatory lockdowns during the COVID-19 pandemic prevented employees from returning to office, many were unable to access the business-critical data and applications they needed to do their jobs. Without a disaster recovery system in place—essentially, a backup plan—availability can be severely impacted in situations like:

- Natural disasters
- Power outages
- Deliberate cyberattacks, like denial-of-service (DoS) attacks or ransomware

Man-in-the-middle attacks

Man-in-the-middle attacks (MITM) involve a malicious attacker trying to intercept, surveil or modify communications between two parties by spoofing one or both party's identities and injecting themselves in-between. Types of MITM attacks include:

- IP address spoofing is where the attacker hijacks routing protocols to reroute the targets traffic to a vulnerable network node for traffic interception or injection.
- Message spoofing (via email, SMS or OTT messaging) is where the attacker spoofs the identity or carrier service while the target is using messaging protocols like email, SMS or OTT (IP-based) messaging apps. The attacker can then monitor conversations, launch social attacks or trigger zero-day-vulnerabilities to allow for further attacks.
- WiFi SSID spoofing is where the attacker simulates a WIFI base station SSID to capture and modify internet traffic and transactions. The attacker can also use local network addressing and reduced network defenses to penetrate the target's firewall by breaching known vulnerabilities. Sometimes known as a Pineapple attack thanks to a popular device. See also Malicious association.
- DNS spoofing is where attackers hijack domain name assignments to redirect traffic to systems under the attackers control, in order to surveil traffic or launch other attacks.
- SSL hijacking, typically coupled with another media-level MITM attack, is where the attacker spoofs the SSL authentication and encryption protocol by way of Certificate Authority injection in order to decrypt, surveil and modify traffic.

Phishing

Phishing is the attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users. Phishing is typically carried out by email spoofing, instant messaging, text message, or on a phone call. They often direct users to enter details at a fake website whose look and feel are almost identical to the legitimate one. The fake website often asks for personal information, such as login details and passwords. This information can then be used to gain access to the individual's real account on the real website.

Preying on a victim's trust, phishing can be classified as a form of social engineering. Attackers can use creative ways to gain access to real accounts. A common scam is for attackers to send fake electronic invoices to individuals showing that they recently purchased music, apps, or others, and instructing them to click on a link if the purchases were not authorized. A more strategic type of phishing is spear-phishing which leverages personal or organization-specific details to make the attacker appear like a trusted source. Spear-phishing attacks target specific individuals, rather than the broad net cast by phishing attempts.