Cybercrime

What is Cybercrime?

Cybercrime is a type of crime involving a computer or a computer network. The computer may have been used in committing the crime, or it may be the target. Cybercrime may harm someone's security or finances.

Think About It...

How do online cyber criminals try to get your data and personal information?

Type your answer here.

Common Online Threats

Phishing

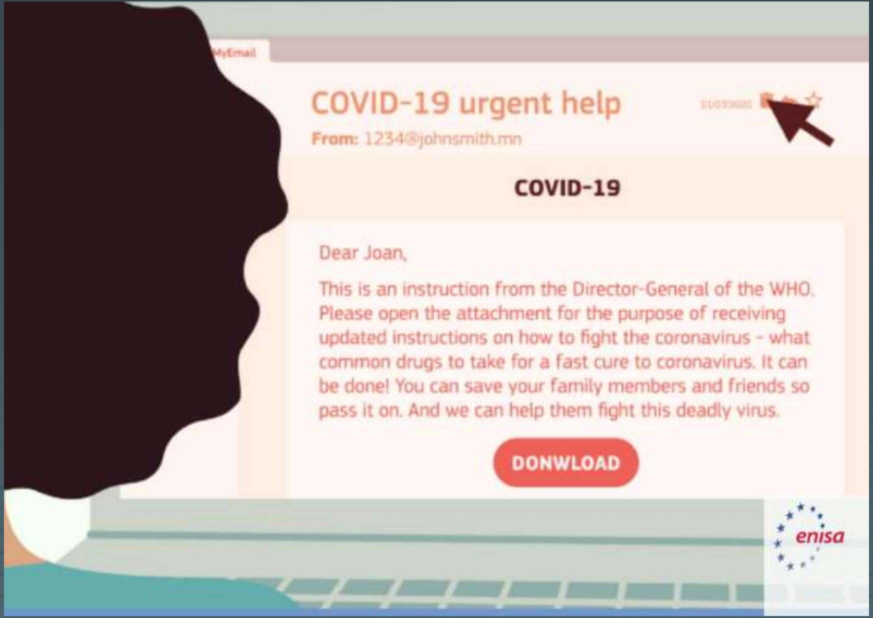
Phishing is the fraudulent practice of sending emails or other messages that appear to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Phishing sites have used target brand names and identities in their website addresses. Amazon was the most targeted brand in the second half of 2020. Paypal, Apple, WhatsApp, Microsoft Office, Netflix, and Instagram were using stolen passwords within four hours of phishing a victim. Some attacks even occurred in real time to enable the capture of multi-factor authentication (MFA) security codes.

Phishers tried to make fraudulent sites appear as genuine as possible.

Pandemic-Related Phishing Example

Notice the misspelling the the word, “Download” on the button.



COVID-19 urgent help

From: 1234@johnsmith.mn

COVID-19

Dear Joan,

This is an instruction from the Director-General of the WHO. Please open the attachment for the purpose of receiving updated instructions on how to fight the coronavirus - what common drugs to take for a fast cure to coronavirus. It can be done! You can save your family members and friends so pass it on. And we can help them fight this deadly virus.

Ransomware Attacks

Ransomware is a type of malicious software from crypto-virology which threatens to publish the victim’s data or block access to data unless a ransom is paid. Ransomware prevents you from accessing your computer (or the data that is stored

Petya is ransomware first discovered in 2016. It infects the computer’s master boot record (MBR), overwrites the Windows bootloader and triggers a restart. Upon startup, the payload encrypts the Master File Table of the NTFS file system and then displays a ransom note demanding payment in Bitcoin.

Pop-Ups

Pop-Ups are unsolicited content that often appear on websites. Usually commercial in nature, pop-ups can also be linked to malware, viruses, and other undesirable content.

Clicking on a malicious pop-up will often download malware or a virus on the user's computer, exposing their personal information.

Scams

Scams are fraudulent schemes or deceptive acts designed to trick individuals or organizations into providing money, personal information, or other valuable assets under false pretenses.

Spam

Spam is an unsolicited message that is sent online to a large number of users. Spam is usually sent for the purpose of advertising, phishing, or spreading viruses or malware.

Sorting Activity

Sort the descriptions at the bottom into the appropriate type of online threat. You should click and drag the description under the appropriate online threat.

Scams	Ransomware	Pop-Ups	Phishing	Spam

A type of malicious software that threatens to block the victim’s access to data unless a ransom is paid.

Unsolicited content that often appears on websites. May be commercial in nature but may also be linked to undesirable content.

Unsolicited messages that are sent online to a large number of users for the purpose of advertising, phishing,spreading malware.

Fraudulent schemes or deceptive acts designed to trick people into providing money, personal information, etc. under false pretenses.

Sending electronic communications in an attempt to obtain personal details by claiming to be from a legitimate source.

Other Cybercrime Examples

Other Cybercrime Examples

- Identity theft
- Spreading hate/inciting terrorism
- Grooming
- Hacking
- Harassment

Online Personal Data

What is Online Personal Data?

Online personal data is the information that individuals willingly or unknowingly share or generate while using the internet or digital platforms.

This data is collected, stored, processed, and sometimes shared by companies for various purposes, including targeted advertising, personalization, analytics, and user profiling.

Safeguarding online personal data is essential for privacy protection and preventing misuse or unauthorized access.

Examples of Online Personal Data

- Names
- Addresses
- Phone numbers
- Email addresses
- Social media profiles
- Financial details
- Login credentials
- Browsing history
- Online purchases

Digital Footprint

A digital footprint is a unique set of traceable digital activities, actions, contributions, and communications. Essentially, a digital footprint is a unique record of a user’s online activity.

Your digital footprint will show where you’ve been on the internet and the data you’ve left behind.

Digital footprints, or records of our data, are useful for people like data brokers and advertisers. They are also useful for hackers and cybercriminals looking to learn more about us, what we are interested in, or to steal our identity.

Protecting Your Data

Avoid using public wifi networks for sensitive activities.

Ensure online social media accounts are set to private.

Don’t give away personal data.

Install anti-virus software on all devices

Avoid clicking on suspicious links.

Use strong and unique passwords.

Enable two-factor authentication

Scenario 1

Riley, a curious teenager, stumbles upon a pop-up ad claiming they've won a free gaming console. Excited, Riley clicks on the ad, which takes them to a suspicious website. Despite warnings from their antivirus software, Riley downloads the supposed "prize." Unbeknownst to Riley, the download contains malware that infects their computer, compromising personal data and giving hackers access to their online accounts. Riley's banking information gets stolen, leading to financial losses and identity theft.

What did Riley do wrong?

Type your answer here.

Scenario 2

Olivia, an enthusiastic social media user, loves sharing her life with her followers. She posts about her vacation plans, upcoming events, and even shares pictures of her credit card for a fun "guess the digits" game. Her extensive sharing catches the attention of a cybercriminal who manages to piece together her personal information from various posts. Olivia's lax privacy settings allow the cybercriminal to learn about her schedule and whereabouts. Exploiting her predictable patterns, they break into her house while she's away on vacation, causing significant property damage and theft.

What did Olivia do wrong?

Type your answer here.

Scenario 3

Tyler, an aspiring entrepreneur, is thrilled when he receives an email from an investor expressing interest in his startup. The email contains an attachment labeled "Business Proposal." Eager to impress, Tyler downloads the attachment without verifying the sender's identity. Unbeknownst to him, the attachment contains ransomware that encrypts his company's critical files. A message appears demanding a hefty ransom in exchange for the decryption key.

What did Tyler do wrong?

Type your answer here.

The Dark Web

What is the Dark Web?

Parts of the internet cannot be indexed by search engines. These parts are referred to as the dark web. You cannot access the dark web through a normal browser.

These are places on the internet where everything is a secret and you can buy and sell anything (legal and illegal) with complete anonymity. The dark web is not regularly monitored by local police, although there are special task forces and teams set up to track dark web activity.

People communicate with each other on the dark web using encrypted messages.

There are legitimate uses for the dark web’s anonymity and privacy (secure communication, whistleblowing, evading censorship in oppressive regimes). However, due to its secrecy and anonymity, the dark web is a very dangerous place full of criminal activity.

Lesson Reflection

Answer the questions below to demonstrate your learning.

What are some common red flags to watch out for when receiving unsolicited emails or messages, and how can you determine their legitimacy before clicking on any links or attachments?	Suppose you come across a website that offers free software downloads that are usually paid. What steps should you take to assess the credibility and safety of the website before deciding to download anything?	You receive a text message with a link claiming to be a special limited-time offer from a popular online store. The message insists that you click the link immediately to claim your discount. How would you evaluate the authenticity of this message and decide whether it's safe to click on the link?
Type your answer here.	Type your answer here.	Type your answer here.