How to protect yourself from cybercrime

What is cybercrime?

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

What are the types of cybercrime?

- Email and internet fraud
- Identity fraud (where personal information is stolen and used)
- Theft of financial or card payment data
- Theft and sale of corporate data
- Cyber extortion (demanding money to prevent a threatened attack)
- Ransomware attacks (a type of cyber extortion)
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own)
- Cyberespionage (where hackers access government or company data)
- Interfering with systems in a way that compromises a network
- Infringing copyright
- Illegal gambling
- Selling illegal items online
- Soliciting, producing or possessing child pornography

Cybercrime involves one or both of the following:

- Criminal activity targeting computers using viruses and other types of malware.
- Criminal activity using computers to commit other crimes.

Cybercriminals that *target* computers may infect them with malware to damage devices or stop them from working. They may also use malware to delete or steal data. They may also stop users from using a website or network or prevent a business from providing a software service to its customers, which is called a Denial-of-Service (DoS) attack.

Cybercrime that uses computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images.

Cybercriminals are often doing both at once. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognize a third category of cybercrime which is where a computer is used as an accessory to crime. An example of this is using a computer to store stolen data.

Examples of cybercrime

Here are some famous examples of different types of cybercrime attacks used by cybercriminals:

Malware attacks

A malware attack is where a computer system or network is infected with a computer virus or other type of malware. A computer compromised by malware could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts or causing damage to data.

A famous example of a malware attack was the WannaCry ransomware attack, a global cybercrime committed in May 2017. WannaCry is a type of ransomware, malware used to extort money by holding the victim's data or device to ransom. The ransomware targeted a vulnerability in computers running Microsoft Windows.

When the WannaCry ransomware attack hit, 230,000 computers were affected across 150 countries. Users were locked out of their files and sent a message demanding that they pay a Bitcoin ransom to regain access.

Worldwide, the WannaCry cybercrime is estimated to have caused $4 billion in financial losses. To this day, the attack stands out for its sheer size and impact.

Phishing

A phishing campaign is when spam emails, or other forms of communication, are sent with the intention of tricking recipients into doing something that undermines their security. Phishing campaign messages may contain infected attachments or links to malicious sites, or they may ask the receiver to respond with confidential information.

A famous example of a phishing scam took place during the World Cup in 2018. According to our report, 2018 Fraud World Cup (the World Cup phishing scam) involved emails that were sent to football fans. These spam emails tried to entice fans with fake free trips to Moscow, where the World Cup was being hosted. People who opened and clicked on the links contained in these emails had their personal data stolen.

Another type of phishing campaign is known as spear-phishing. These are targeted phishing campaigns which try to trick specific individuals into jeopardizing the security of the organization they work for.

Unlike mass phishing campaigns, which are very general in style, spear-phishing messages are typically crafted to look like messages from a trusted source. For example, they are made to look like they have come from the CEO or the IT manager. They may not contain any visual clues that they are fake.

Distributed DoS attacks

Distributed DoS attacks (DDoS) are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected IoT (Internet of Things) devices are used to launch DDoS attacks.

A DDoS attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests. Cybercriminals who are carrying out cyberextortion may use the threat of a DDoS attack to demand money. Alternatively, a DDoS may be used as a distraction tactic while another type of cybercrime takes place.

A famous example of this type of attack is the 2017 DDoS attack on the UK National Lottery website. This brought the lottery's website and mobile app offline, preventing UK citizens from playing. The reason behind the attack remains unknown, however, it is suspected that the attack was an attempt to blackmail the National Lottery.

Impact of cybercrime

Generally, cybercrime is on the rise. According to Accenture's State of Cybersecurity Resilience 2021 report, security attacks increased 31% from 2020 to 2021. The number of attacks per company increased from 206 to 270 year on year. Attacks on companies affect individuals too since many of them store sensitive data and personal information from customers.

A single attack – whether it's a data breach, malware, ransomware or DDoS attack - costs companies of all sizes an average of $200,000, and many affected companies go out of business within six months of the attack, according to insurance company Hiscox.
Javelin Strategy & Research published an Identity Fraud Study in 2021 which found that identity fraud losses for the year totaled $56 billion.

For both individuals and companies, the impact of cybercrime can be profound – primarily financial damage, but also loss of trust and reputational damage.

How to report a cybercrime

Reporting a cybercrime in the US:

File a report with the Internet Crime Complaint Center (IC3) as soon as possible.
Visit ic3.gov for more information.

How to protect yourself against cybercrime

Given its prevalence, you may be wondering how to stop cybercrime? Here are some sensible tips to protect your computer and your personal data from cybercrime:

Keep software and operating system updated
Keeping your software and operating system up-to-date ensures that you benefit from the latest security patches to protect your computer.

Use anti-virus software and keep it updated
Using anti-virus or a comprehensive internet security solution like Kaspersky Total Security, is a smart way to protect your system from attacks. Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you peace of mind. Keep your antivirus updated to receive the best level of protection.

Use strong passwords
Be sure to use strong passwords that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

Never open attachments in spam emails
A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

Do not click on links in spam emails or untrusted websites
Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.

Do not give out personal information unless secure

Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.

Contact companies directly about suspicious requests

If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal. Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialed, they can pretend to be from the bank or other organization that you think you are speaking to.

Be mindful of which website URLs you visit

Keep an eye on the URLs you are clicking on. Do they look legitimate? Avoid clicking on links that are unfamiliar or URLs that look like spam. If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.

Keep an eye on your bank statements

Spotting that you have become a victim of cybercrime quickly is important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent or legitmate.