From Antivirus to Zero-day exploit:

20 cybersecurity terms you need to know

NordVPN®

“

Cybersecurity touches everything we do online and now more than ever, online life is normal life. By extension, cybersecurity threats are threats to our livelihoods and educating ourselves is essential for protecting our wellbeing. Everyone benefits from understanding the basics which is why the A-Z of cybersecurity terms is important for all of us to understand.

Troy Hunt

Advisory Board Member at NordVPN, a Microsoft Regional Director and Most Valuable Professional awardee for Developer Security, blogger at troyhunt.com, international speaker on web security and the author of many top-rating security courses for web developers on Pluralsight.

Foreword

If you're taking your first steps into the realm of cybersecurity, this is the place to start. To explain why, let's see how things usually work.

You've come across the word spyware, and you want to know what it means. The moment you start looking, you're assaulted by terms you've never heard before. You may find a definition like this:

> Spyware is a type of malware that monitors the victim's device to extract sensitive data without the victim's knowledge. Examples of spyware: adware, keyloggers, and trojans.

That's an accurate definition, but it's not super helpful. Now you have more questions. How does spyware work? What is considered sensitive data, and how worried should you be about its security? What's a keylogger? Is that even a word?

We're taking a different approach.

Rather than giving technical definitions, we're going to show how cybersecurity affects your life and provide down-to-earth comparisons. This is not a comprehensive glossary, and it's so by design. It's meant to whet your appetite for further learning.

If you're looking for more detailed, technical explanations on all things online security, try our blog at NordVPN.com/blog, which provides both popular and in-depth content.

Table of contents:

3 Antivirus

4 Botnet

5 Ciphertext

6 Data breach

7 End-to-end encryption

8 Firewall

9 Hacker

11 IP address

12 Cryptojacking

13 Keylogger

14 Logic bomb

15 Man-in-the-middle-attack

16 Network

17 Phishing

18 Ransomware

19 Social engineering

21 Two-factor authentication

22 VPN

23 Wi-Fi

24 Zero-day-exploit

Antivirus

You got a new email. Subject: **I love you**

In it, you find a beautiful confession of love from an anonymous admirer. And there's a photo too. Curious, you click on the attachment — and download a virus.

Your antivirus immediately quarantines it. You got lucky — it was an old virus, its signature already in the database.

If the virus is new and not registered in the database, the antivirus can use other tools to detect it. It monitors your computer for suspicious activity. If a program tries to bypass the antivirus, runs on startup without permission, or downloads other malware, the antivirus reacts.

And it's not only viruses. There are all kinds of malicious software — trojans, ransomware, keyloggers, etc. — that try to compromise or abuse your devices.

Today, the word "antivirus" stands in for all kinds of anti-malware tools that protect devices from malware.

Related terms: virus, malware, anti-malware software, trojan, worm, adware.

B

Botnet

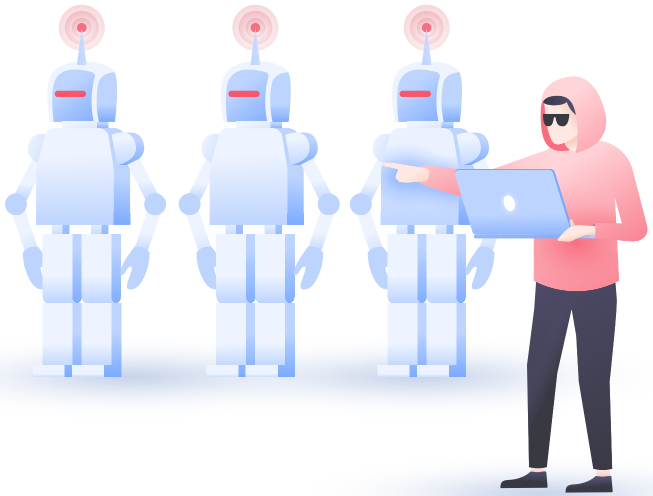
You open your browser, enter the address of your favorite meme website. Awww, it’s down. And you’ll never guess why.

It’s zombies.

Bots, to be exact. A swarm of mindless, infected devices have sent hundreds of thousands of requests to the website and overwhelmed it.

This attack is called DDoS, which means distributed denial of service. People use botnets for this and other nefarious purposes, like email spam or creating fake internet traffic.

Your devices may also be part of a botnet, secretly responding to cybercriminal’s commands. It’s hard to know whether your computer is a bot — the only sign may be a slightly worse performance or overheating.



Related terms: bot, zombie, DDoS attack.

Ciphertext

You open a messaging app and text, “SORRY GUYS, can’t make it tonight. Probably caught a stomach bug.”

That’s called plaintext. It’s unencrypted text that can be intercepted and read by an online spy. That’s also called a lie — you feel fine, but you’d rather watch a movie.

At least you’re using a secure messaging app. It applies an algorithm to turn your lie into ciphertext:

“ueEeQrwrd1GL24HWDi2ttNg5flUXUzqslFqb94^Ef2NU1NBrD rPb84wbReVnclTP2AgnMCkhaHC3UrfR8VWxh3jWWh+0WE”

That’s encryption in action. Plaintext is turned into ciphertext via a secure key (a cipher). The messaging apps your friends use have the key that deciphers your messages. Online spies don’t have the key and can’t read your communications.

eEeQrwrd1GL24HWDi2ttNg5flUXUzqsl/skFDqb94sCvbWGZlYnLk8h
qsl/skFDqb94sCvbWGZlYnLk8hhaSEfCkham

Related terms: encryption, cipher, plaintext, decipher.

D

Data breach

You have a group chat with a bunch of your closest friends. One day, you notice screenshots from the chat circling all over social media. You've just experienced a data breach.

A data breach happens when sensitive data falls into the hands of someone who has no business handling it.

How did this happen? A hacker intercepted your communications? Or was it an inside job? Perhaps Mark's roommate accessed the chat while Mark was away from the laptop. He always looked shady. You'll probably never find out.

That's what happens in major corporate data breaches too.

Companies collect vast amounts of data — sometimes data from users like you — and some of these companies get breached, the data is leaked, and you see your logins and passwords floating around the web.

Periodically check whether your accounts have been compromised in a data breach on haveibeenpwned.com.

Related terms: unintentional information disclosure, data leak, data spill.

End-to-end encryption

You've heard it said in a joyous tone: "We'll be implementing end-to-end encryption!" What's so end-to-end about it?

Think of your data as a paper note. Before sending it out, you put it in an envelope, which protects its contents from eavesdroppers. That's encryption.

Somewhere along the way, a third party (for example, the instant messaging service you're using) opens that envelope, takes out your data, and sends it to the final destination.

That's just how the internet works — there are middlemen all the way down.

End-to-end encryption cuts out the middleman. Only you and the person you're sending the note can see its contents.

Related terms: ciphertext, plaintext.

F

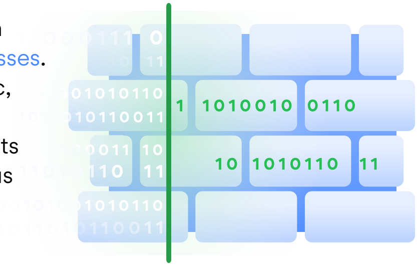
Firewall

You're standing in a line. When you reach the bouncer, he says, "No entry." You turn back and head home — no clubbing today.

The bouncer enforces the rules on who gets into the club and who doesn't. These rules are arbitrary — they depend on the club's policies and external circumstances. For example, the club is full, or it's hosting a private party.

In the same vein, a firewall stands between your local network and the internet. Like a digital bouncer, it enforces the rules on which traffic is good enough to enter your network.

A firewall allows traffic from trusted sources or IP addresses. Not on the list? Sorry, traffic, turn back and head home. That's how a firewall protects your network from malicious internet traffic that could compromise your system.



Hacker

You've met them in movies. Mysterious, dangerous, even anti-social. They're digital outlaws who live off the grid. They hack the Pentagon in under 5 minutes.

That's clearly fiction. Hackers are people — and every person has their motives. Some enjoy the intellectual challenge of breaking into networks. Others, the so-called black hat hackers, act with malice. They compromise systems for personal gain, steal valuable data or money, disrupt networks, and may cause all kinds of damage.

Many companies and governments employ white hat hackers, who test the security of their computer systems by trying to break in. That's called penetration testing, which can take many forms — even physical.

For example, a white hat hacker may enter the company building by following an employee. People are polite — they usually hold the doors open for others, even strangers. Once inside, the hacker may steal hard drives with sensitive data, access unsupervised computers or compromise them (with keyloggers, for example).

Can you get hacked?

It depends on your security measures. However, extremely skilled hackers often find a way into the most secure networks. The good news is that they probably have for juicier targets on their mind than your Steam account.

Usually, you suffer from hackers indirectly, see: data breach.

What you should be wary of are scammers who set up fake websites and send malicious links, see: phishing. Enter your password on a scam website — and you're giving it directly to the scammer.

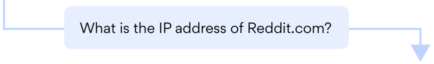
Related terms: grey hat hacker, black hat hacker, white hat hacker, penetration, penetration testing.

IP address

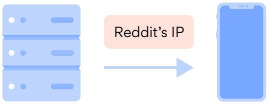
Your phone has an IP address (short for internet protocol address) assigned by your network. So does your laptop, smart TV, and other every gadget that connects to the internet. No device could function online without one. Why?

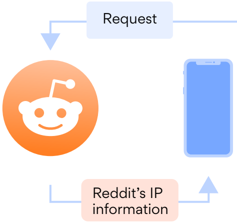
Let's say you need to kill some time. You take out your phone and type in "Reddit.com" in the address bar.

But your phone doesn't know what "Reddit.com" means. Numbers, not words, are its native language. To access Reddit, your phone sends out a question: "What is the IP address of Reddit.com?"



The question is addressed to a special server — a database of IP addresses. The server finds Reddit's IP and sends it back to your phone.





Your phone then sends out the request to Reddit's IP address. Reddit sends back the information to your phone's IP.

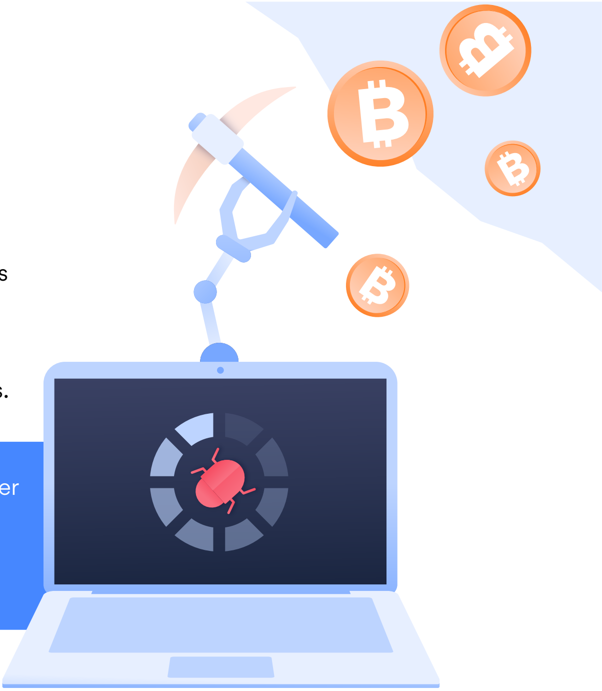
A second passes. Reddit loads on your screen. Meh, nothing sparks your interest, you hit the close button.

J

Cryptojacking

Your computer is hot and buzzing, the fan is spinning like crazy. And it's slow — you have to wait a while before anything loads.

The reason? A hacker has hijacked your computer to mine cryptocurrency.



You've probably heard of cryptomining. To put it simply, it's when you receive cryptocurrency as a reward for running complex calculations on your computer. But these calculations take up a lot of computer power — usually too much power for cryptomining to be profitable.

To solve this problem, hackers hijack devices to mine cryptocurrency for them. They perform this attack — called cryptojacking — by using malware or malicious code in web pages.

Unsuspecting victims are left to wonder why their computer is red hot from overheating.

P.S. Yes, we know that putting cryptoJacking under J is cheating. But the letter J is an empty desert when it comes to cybersecurity terms, so we abused it.

Related terms: cryptomining, malicious cryptomining.

Keylogger

You're in the library, writing a paper for your economics class. It's due yesterday. Your laptop battery dies, and you've left the cord at home.

A friendly-looking girl is sitting nearby. You ask for her laptop — you need 5 minutes to finish the thought while it's still bubbling in your head. She's glad to be of help. You take her laptop, log into your cloud drive, and finish the critique of Depression-era antitrust policies.

When you get back home, you find that your email and a lot of your online accounts have been hacked. How?

The girl had a keylogger installed on her laptop. It's a tool that registers keystrokes. It recorded everything you typed, including your cloud drive password and login.

Since you use the same password for your cloud drive and email, the hacker gained access to your primary email account (that's why you shouldn't reuse passwords). With it, she reset the passwords of your other accounts.

Keyloggers rarely come from friendly-looking girls. Usually, they take the form of hardware gadgets that hackers attach to unsupervised computers. They can also be software tools, used both illegally or legally. For example, some corporations install keyloggers in their computers to monitor their employees.

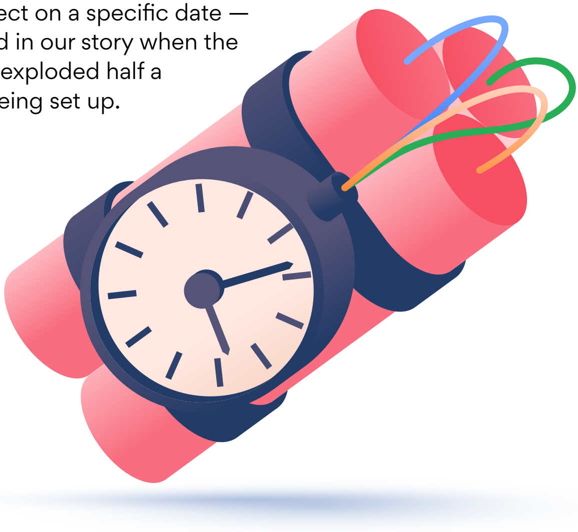
Related terms: spyware.

Logic bomb

You're at work, five minutes past a deadline. You’re typing furiously when everything crashes. You can’t access the internal network or any remote files. No more work today.

The next day, you hear rumors. It was a former employee, a disgruntled IT guy — he shut down the internal network. But how can that be? He was fired half a year ago and had no more access to the company’s systems.

Well, on his last day at work, he left a logic bomb. It is a piece of malicious code that activates when certain conditions are met. For example, when the CEO logs into a sensitive system. A logic bomb can take effect on a specific date — as happened in our story when the logic bomb exploded half a year after being set up.



Related terms: time bomb, insider threat.

Man-in-the-middle attack

You’re in a coffee shop, connected to the public Wi-Fi. You’ve just sent an email to your contractor, asking for their bank account number. You get the number, pay the fee, drink the flat white.

Two days later, the contractor calls you with a question: “When will I get paid?”

What?

Flashback to the coffee shop. A hacker arrived at the coffee shop before you, set up an evil twin hotspot, and named it “Coffee shop FREE wifi.” Believing it’s a legitimate network, you connected to it. From that moment on, the hacker could monitor your internet traffic.

That's a man-in-the-middle attack in action.

The hacker intercepted your email and sent you his own bank account number. He got paid, while the contractor is still waiting for the fee.

Keep in mind the public Wi-Fi is not a safe network. Even if it’s not set up by a hacker, you never know how well it’s configured. A man may be lurking in the middle of your communications. Make sure you use a VPN before connecting to one.

Related terms: evil twin attack, Wi-Fi honeypot.

N

Network

Your devices are a part of a network, which is a part of a bigger network, which may be a part of an even bigger network, which — you get the idea. That’s the internet, a network of computer networks, big and small. And you’re on it.

The network that’s closest to you is called LAN — local area network. It refers to a group of interconnected devices in one physical location. So when you connect to your home router, you connect to your LAN.

Your home network is probably quite small, up to 10 connected devices (or if you love gadgets, a lot more — but we’re not judging, tech is awesome). A LAN can also be company-wide, or it can cover the whole school with thousands of interconnected devices.

Related terms: internet, LAN.

Phishing

You get an email from your bank. It's a warning — someone tried to withdraw money from your account. "Please send your login and password IMMEDIATELY to confirm your identity," the bank says.

Sounds scary, but you shouldn't act out of fear.

Carefully check the sender and you'll probably find it's not your bank, but someone impersonating it. Do not reply, do not click on any links in the email. Call your bank directly and ask about the email.

The scam is called phishing and takes on many forms. Messages or emails that use fear and urgency to extract confidential details. A fake website that looks almost exactly like your university's. Enter your login and password and you're giving them away to a scammer.

The defense is simple — be cautious. Be wary of fishy messages that play on your fears or even worse — promise something too good to be true. By the way, you've
a click here to claim them.

Stop, think, and double-check. Do not click on a link if the URL doesn't look legitimate. As a general rule, never enter or disclose your password unless you're absolutely sure it's safe.

R

Ransomware

You turn on your computer and — wait, what's this? The screen does not load. But there's a message: "Your files have been encrypted by NarutoRun Hacker Group. You have one week to transfer $500 in Bitcoin to our wallet, or your files will be gone forever. Rasengan!"

Sounds like a plot of a poorly written comedy, but it's no laughing matter. Ransomware is a type of malware that forcibly encrypts the victim's data. Nobody but the hackers can undo the encryption because only they hold the key. (There are plenty of encryption protocols that are practically unbreakable without the decryption key. See: ciphertext, end-to-end encryption.)

You shouldn't pay the ransom because your dollars (more likely — cryptocurrency, usually requested by hackers) would only support criminals. Instead, learn how to fight ransomware:

- Don't download anything from suspicious websites. Don't open suspicious links, emails, or messages. See: phishing.
- Back up your most sensitive files.
- Update your apps and software, especially your security software.
- Use strong passwords.

Social engineering

You are woken up by your phone in the early morning. The person on the other end politely explains he's a technician at LiteNet, your internet service provider. They have experienced a network failure that may have resulted in minor data loss.

Could you provide that last four digits of your credit card number, so that they could match them with the records on their servers?

Half asleep, you do so and get back to your dreams. You properly wake up two hours later, eat a huge breakfast, and find that you've been hacked.

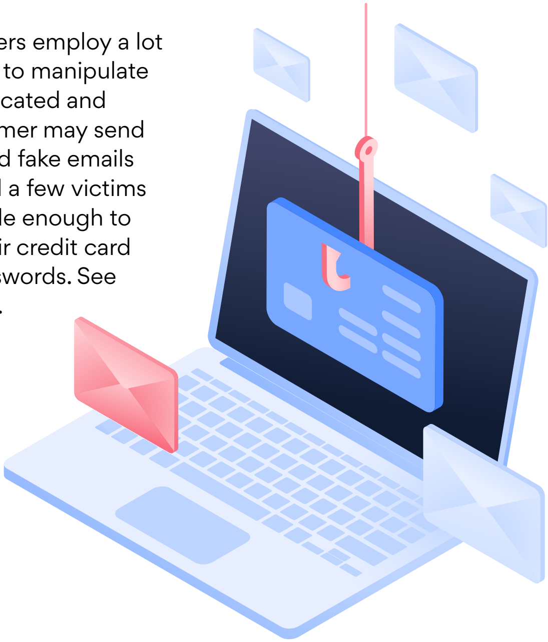
The person who called you was no technician, but a social engineer — a scammer who uses psychological manipulation to trick people into performing a specific action or revealing sensitive details.

Let's break it down. The scammer caught you early in the morning, introduced himself to alleviate your suspicions (LiteNet is the biggest internet provider in your area, it was an easy guess), and dropped some meaningless technical jargon to sound legitimate.

Then he called LiteNet pretending to be you and said he'd forgotten his password. He provided the last four digits of your credit card number to confirm identity (that is — your identity) and reset your LiteNet password — including the password for your LiteNet email account.

LiteNet is a fake internet provider we created for this story. But many real companies may reset your password over the phone based only on the last four digits of your credit card. You should provide as little sensitive information as possible when signing up and explicitly state not release any details over the phone.

Social engineers employ a lot of techniques to manipulate users, sophisticated and blunt. A scammer may send out a thousand fake emails hoping to find a few victims that are gullible enough to reply with their credit card details or passwords. See also: phishing.



Two-factor authentication

You're logging into Twitter on your friend's phone because you left yours at home. Since this is a new device, you need to confirm the login on a special authentication app. Which is on your phone. Which is at home.

Aargh, it's cybersecurity catch-22!

Yes, it may cause you slight inconvenience, but two-factor authentication (2FA) secures you with a second layer of protection. If you have trouble accessing your account without your phone, so will the hackers.

The two factors usually are:

Something you know (a password or a pin code).
Something you have (a phone, a codebook, or your biometrics).

No system is impregnable, but 2FA upgrades the security of your accounts to a level beyond what most users have. Cybercriminals are usually opportunistic, so instead of trying to work around 2FA, they'll choose other targets, preferably someone you uses ABCDEFG as their password.

You should enable 2FA on all services that support it. It's an easy way to be much more secure online with minimum inconvenience.

Related terms: multi-factor authentication.

V

VPN

You browse, you scroll, you surf. And every time you go online, you leave bits of data about yourself. Your internet service provider has access to your online traffic. Every website you visit can see your IP address.

It's not just privacy, but your online security that's also at stake. A lot of websites still do not use a secure communication protocol. Most apps do not disclose what kind of cybersecurity practices they employ. You're left with having to trust them without grounds to do so.

A VPN (virtual private network) is a tool that directs all your traffic through a secure server, encrypts it in the process, and changes your IP and virtual location. Even though it may sound technical, VPN is a mainstream tool that's easily accessible for laymen.

It doesn't mean that all VPNs are equally good. A VPN routes all your traffic through its servers, so it may collect your data and sell it to the highest bidder. The good news is that most of the biggest VPNs are transparent about their practices, keep no user logs, and so have nothing to sell or disclose to third parties.

For example, we at NordVPN have our no-logs policy and service regularly assessed by a Big Four auditing company.

Related terms: time bomb, insider threat.

Wi-Fi

You’re in your hotel room, browsing on the free Wi-Fi. A few floors down, a hacker is spying on your online activity. How?

Public Wi-Fi is inherently unsafe — cybercriminals can use many methods to exploit or compromise it.

If the router is poorly configured, a hacker could observe the internet traffic of anyone using the public hotspot. Or the hacker may find a way to inject malware over the network into your device.

A hacker may set up a fake hotspot — an evil twin — and trick you into connecting to it. See also: Man-in-the-middle attack.

How safe you are depends on:

The configuration and security measures on the hotel Wi-Fi.
The security practices of websites you visit and apps you use.
Your personal cybersecurity practices.

Usually, you can’t know how secure a public network is, so avoid accessing sensitive data when connected to it. Why not switch to mobile data instead? Or turn on a VPN?

P.S. If you’re organizing an event, don’t rely on the Wi-Fi provided by the venue because it’s rarely secure. Properly setting up a Wi-Fi hotspot is no easy task and requires precise technical knowledge — better hire professionals if you don’t have the technical skills.

But your job is just as important — you need to communicate! Inform the attendees of the event about the official hotspots and warn them not to connect to any other hotspots, even if they seem legitimate.

Related terms: malware injection, Wi-Fi sniffing.

Z

Zero-day exploit

You updated your software, installed an antivirus, turned on your firewall. At this moment, no hacker could break into your system, right?

If only it were that simple.

Computer networks, software, and hardware are created by people. People make mistakes, they do not think through every possible scenario, they leave vulnerabilities.

Hackers exploit them. They look for the weakest link in the system and break it.

As soon as a vulnerability is discovered, it's patched. The updates you install for your apps or operational system are often just that — patches for newly discovered vulnerabilities.

(Of course, some vulnerabilities can never be patched. Humans, not machines, are often the weakest link when it comes to cybersecurity. See: social engineering.)

A zero-day vulnerability is unknown to the vendor, and so it hasn't been patched. The name refers to the number of days a vendor had to fix the vulnerability — zero. An attack based on this vulnerability is called a zero-day exploit or zero-day attack.

So even if you keep your system secured, patched, and updated, a zero-day exploit may compromise it through a previously unknown vulnerability. The solution is constant vigilance. Be smart when online, use strong passwords, don't click on links if you're not sure they're safe.

This way, you'll minimize your risks and force cybercriminals to look for easier targets.

Related terms: zero-day vulnerability, zero-day attack.