Cloudwards

Cybersecurity & Encryption 101

The Complete Guide to
Cybersecurity & Encryption

Course by Cloudwards

Benefits:

- Learn simple, effective ways to keep yourself safe in a connected world.
- Separate the truth from the marketing hype when shopping for VPNs and antivirus.
- Avoid the common mistakes that lead to 80% of cyberattacks.

What you'll learn:

- Who wants access to your private data, and the tricks they use to get it
- How cryptography has evolved from ancient times to protect the modern internet
- The unseen ways encryption impacts your life
- Secret techniques of security experts and white-hat hackers

Course Content

Welcome to the Cloudwards course on cybersecurity and encryption. We'd like to commend you for embarking on this learning journey. Cybersecurity is a topic that impacts everybody. As the world's economy becomes increasingly dependent on a functioning internet, it's everyone's responsibility to understand how that internet is threatened -- and how to keep it safe.

The free and open internet allows people worldwide to exchange ideas and trade goods and services. However, with new frontiers come new dangers, and government regulations have been slow to catch up. Thus, connecting online often means taking online privacy into your own hands. The better you understand cybersecurity, the more capable you'll be of protecting yourself.

Though cybersecurity and encryption can seem like obscure topics, they're easier to grasp than you might think. If you've ever solved a cryptogram puzzle or turned a note into a code so only your best friend could read it, you've already taken your first steps in the world of encryption.

In these nine chapters, you'll learn how complex math works alongside old-fashioned common sense to protect businesses, governments and people like you from potentially catastrophic cyberattacks. You'll discover how high-profile hacks occurred and how they could have been prevented, as well as how to separate truth from hype when choosing cybersecurity tools.

Here's a quick guide on what you can expect to learn:

- Chapter 1: **Unraveling the Basics of Cybersecurity** gives an overview of the exact threats cybersecurity works to counter and the everyday actions you can take to mitigate your risk online.
- Chapter 2: **Decoding Encryption Techniques** examines the nuts and bolts of encryption -- the science of preventing data from being read by anyone except the intended recipient.
- Chapter 3: **Encryption in Everyday Life** takes the techniques from Chapter 2 and explains how they apply to tasks you use the internet for every day.
- Chapter 4: **The Evolution of Cyberattacks** goes into detail on the rapidly changing world of cyber threats by illustrating three case studies from the last 20 years.
- Chapter 5: **Securing Your Digital Footprint** expands on the advice in Chapter 1 to teach you how to guarantee your own online security.
- Chapter 6: **Cybersecurity in the Workplace** explains how workplaces -- often seen as prime targets for cybercrime -- keep their systems secure.
- Chapter 7: **International Cybersecurity Regulations** covers some of the actions governments have taken to protect online security.
- Chapter 8: **Ethical Hacking and Penetration Testing** explains the vital role security consultants and volunteers play in stress-testing systems and reporting vulnerabilities.
- Chapter 9: **Emerging Trends in Cybersecurity** reveals how cutting-edge technology like AI, blockchain and quantum computing are changing the cybersecurity landscape, and analyzes which new threats and opportunities might emerge as cybersecurity continues to evolve.

We recommend pausing at the end of every chapter to review what you've learned and to check whether there are any concepts you're still unsure about. There won't be a test, but you can start putting these cybersecurity tips into practice as soon as you learn them.

Chapter 1: Unraveling the Basics of Cybersecurity

Security is a pretty simple concept at heart. First, you designate a secure area, such as a lockbox, a private room or a whole building complex. Then, you take steps to make sure nobody can gain access without your knowledge and approval, with the aim of protecting something of value within the boundaries of that secure area.

Of course, it gets much more complex than that. Sometimes several secure areas nest within each other and different people will require varying levels of clearance. You may need to protect a valuable object in transit as it moves from one secure area to another. Perhaps you want to allow free access to an area but retain the right to expel people who break certain rules.

Cybersecurity means applying the principles of security to **cyberspace** -- the entire world of digitally connected devices, from private networks all the way up to the internet itself. It has the same goals as physical security -- to protect things of value -- with one key difference. Since nothing physically exists on the internet, cybersecurity is dedicated to the protection of data.

The Importance of Data Protection

The exchange of data is the backbone of the internet. When you go online, your router sends data for your internet service provider (ISP) to forward to the website you want to visit. The servers storing that website receive your data and send you data in return. A Netflix show, your social media pages and your online bank account are all made of strings of data.

That data is worth a lot of money (in fact, some of it literally represents money). Today's developed economies rely more on information than on manufacturing; many of the biggest industries in the United States make their money by collecting and providing data.

Where there's money, there are people trying to get at it unlawfully. To an unethical internet user, any piece of data represents a potential payoff. Consider a bank account username and password -- just an email address and 10 characters can be worth thousands of dollars in ill-gotten gains.

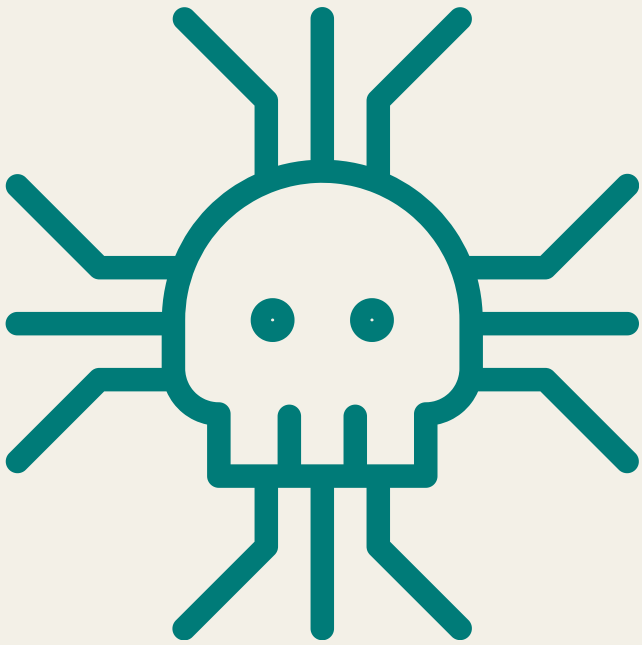
Data privacy is often a right even if the data isn't directly valuable. For example, HIPAA, the Health Insurance Portability and Accountability Act, safeguards patient data because only caregivers need those intimate details. The beauty of the right to privacy is that you never have to explain why you want information to be private. You have the right no matter the reason.

Understanding Cyber Threats

Cybersecurity defends computers and networks against all sorts of threats. However, at their core, nearly all cyber threats are **methods to gain access to a system without permission**.

Even attacks like **DDoS** that seem to do nothing but cause chaos are frequently used as distractions while hackers break into another part of the system.

Why do criminals want to break into secure systems? There are two main reasons: Either they want to gain control of valuable data in those systems, or they want to co-opt the system for another purpose. Let's explore several well-known types of cyber threats in the context of those two motivations.



- **Malware**, short for "malicious software," is a broad term for any program secretly planted on a user's device for nefarious purposes. Malware is often classified by its objectives.
    - **Spyware** secretly records information on your activities.
    - **Adware** displays advertisements.
    - **Ransomware** locks up your files until you pay to get them back.

- A **computer virus** is another type of malware, but the way it replicates is different. Once on a network, a virus replicates itself across all connected devices. In the early days of the internet, hackers released viruses as a form of bragging; today, as cybercriminals' motives shift toward financial gain, true viruses are rare.

- **Social engineering** is another umbrella term. Instead of technical methods, social engineering attacks rely on predicting and manipulating the target's behavior. For example, **phishing** involves posing as a legitimate authority and convincing victims to hand over sensitive data.

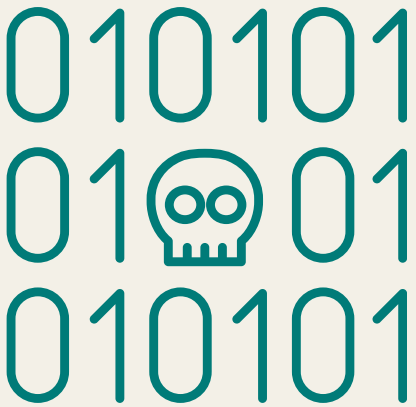
- **Distributed denial of service (DDoS)** attacks can be used to temporarily take down a website. Using a network of corrupted computers called a **botnet**, hackers send the website so many requests that it crashes. Botnets are formed from devices previously infected by malware.

- **Man-in-the-middle (MITM)** attacks occur when hackers insert themselves into online transactions by posing as a component in a legitimate exchange -- an action called **spoofing**. Criminals might spoof websites, WiFi networks, security layers, browser cookies or email accounts.

- **SQL injections** exploit the databases where websites store usernames and passwords. Certain code commands can make the database give up its contents or destroy the database completely.

- **Data breaches** involve hackers gaining access to a database full of user account credentials and making them available on the **dark web**. If a hacker gets your information in a data breach, they can steal your money or impersonate you without having interacted with you at all.

Another factor that unites the various types of cyberattacks is that they're **increasingly less reliant on technical know-how**. Some types of malware are available as **subscription services**, while many social engineering attacks require no computer science knowledge whatsoever. Fortunately, **low-tech methods are just as effective at countering these attacks**.



Best Practices for Online Safety

The key to countering cybercriminals is first to be aware of the methods they use and then to intentionally close off those avenues. This involves a combination of technology and common sense.

The vast majority of hacks occur because of weak, easily guessed passwords. Just like a real-world criminal would rather use a stolen key than break a window, there's no reason for hackers to bother with complicated exploits when they can log in to your sensitive accounts in a seemingly legitimate way.

Some of the most common factors that make passwords guessable include:

- Using any of the 100 or so most common passwords
- Failing to change a device's default password
- Basing passwords on publicly available information like your name or birthday
- Using a short password (five characters or less) that can be guessed in random attempts
- Using the same password on every site

The last bullet point is extremely important and is the reason why data breaches are so dangerous. If you use the same password for every account, your entire identity is only as strong as the weakest site that you've used it on. Venmo may have reliable security, but if you log in with a password that was compromised in a breach elsewhere, your money is still forfeit.

You can foil 80% of cyber threats simply by **using passwords that hackers can't guess**.1 Don't worry, though -- that doesn't mean you have to spend your whole day sorting out 100 different strings of random letters and numbers.

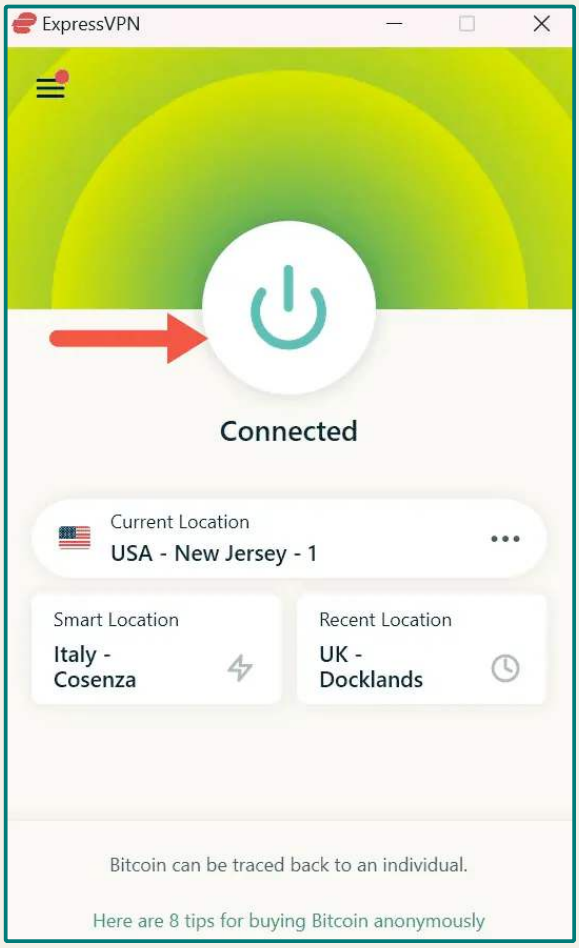
Here are some tricks to make strong passwords a habit:

- **Use a password manager.** A password manager is an app that integrates with web browsers. They can not only generate long passwords on command but can also save those passwords for you and fill them in when you need them. The only password you have to remember is the one that unlocks the password manager itself.
- **Watch the news for reports of data breaches.** If a service you use suffers a data breach, use a resource like HaveIBeenPwned.com or NordVPN's dark web monitor to see if you've been impacted.
- **Don't base your password on information you might share.** In the age of social media, hackers have ways of learning your birthday, your favorite movie and your mother's maiden name. If you have to share personally identifiable information online, make sure it doesn't match any of your usernames or passwords.

Of course, no password is strong enough if a scam artist can trick you into giving it up. **Be extremely skeptical if a stranger ever says they urgently need your password** -- it is likely a hacker attempting a phishing attack. We'll talk more about common-sense methods in Chapter 5: Securing Your Digital Footprint.

Another vital best practice to remember is to **always update software as soon as updates become available**. Software manufacturers frequently issue updates to fix newly discovered vulnerabilities in their code; if you don't update, you might leave yourself vulnerable.

Finally, you can protect yourself against DDoS and MITM attacks by using a **virtual private network (VPN)**. DDoS attacks rely on the hacker knowing your IP address, while MITM attacks depend on the hacker intercepting unencrypted traffic. A VPN hides both your IP address and the requests you send online. We'll discuss VPNs in much more detail in the chapters to come.



ExpressVPN is one example of a simple VPN app that pays massive security dividends.

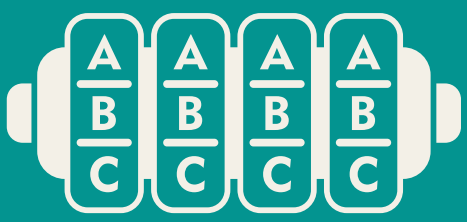
Chapter 2: Decoding Encryption Techniques

After the World Wide Web itself, **encryption** may be the most important technology behind the internet age. It protects both individual rights and business secrets, and makes secure connections between two devices possible.

Yet for such a vital development, encryption is surprisingly simple. It just means **concealing information so only your intended recipient can read it**. Methods of doing so have been employed since ancient times, and examples can be found throughout history and literature.

In the world of encryption, sentences like these ones are called **plaintext**. Anybody can read plaintext if they know the language used to write it. A **cipher**, or an **encryption algorithm**, is a set of rules for turning plaintext into **ciphertext**. The ciphertext should be illegible to anyone who doesn't have the **key** -- the instructions for turning the ciphertext back into plaintext.

There are as many ciphers as there are languages, but those used on the internet tend to fall into one of two categories: **symmetric** or **asymmetric**. The main difference between them is the type of key used. Each of these categories has its own approaches and use cases. When combined, they're the most important tools in modern cybersecurity.



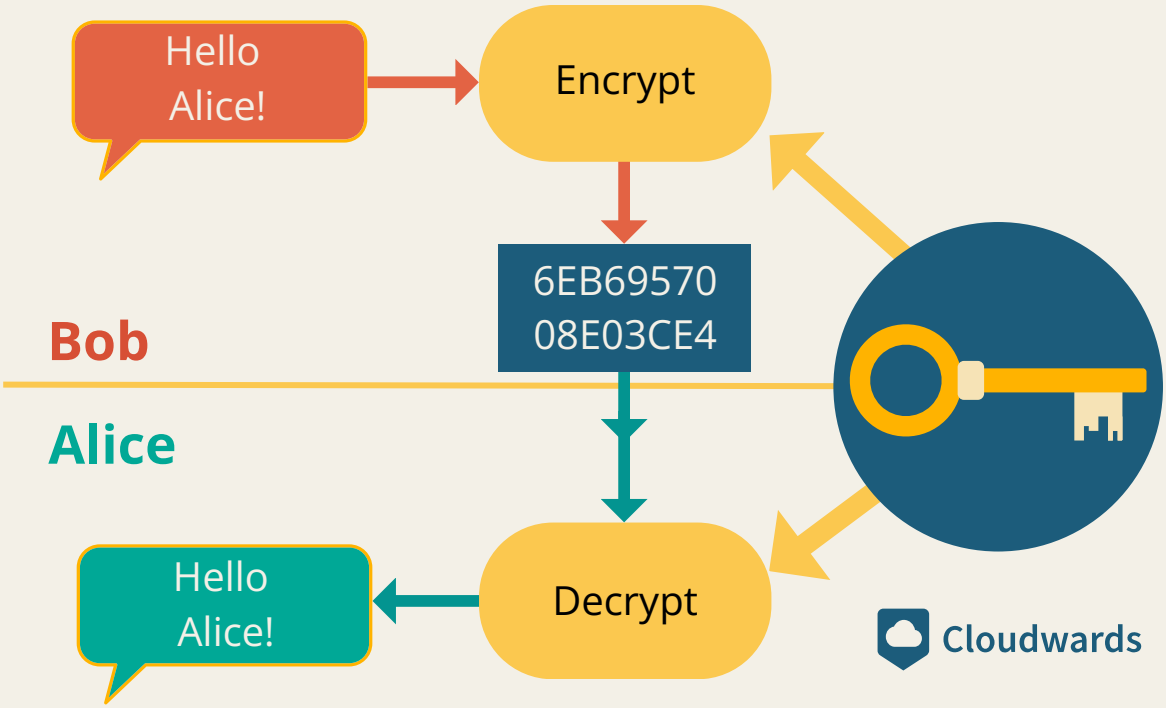
Symmetric Encryption

In symmetric encryption, **the sender and recipient both use the same key**. The cipher uses the key to encrypt the plaintext on one end, and the recipient uses the same key to decrypt the ciphertext. Ciphers can be as simple as shifting each letter two places forward in the alphabet, but most algorithms are more complex to ensure they cannot be decrypted without the key.

Modern symmetric ciphers use one of two approaches. **Block ciphers** encrypt data in blocks of the same size, each with its own key. The **Advanced Encryption Standard (AES)** is the most prominent example.

Stream ciphers encrypt each byte of data as it comes regardless of block size. **RC4** and **ChaCha20**, which the **WireGuard protocol** uses, are the best-known examples.

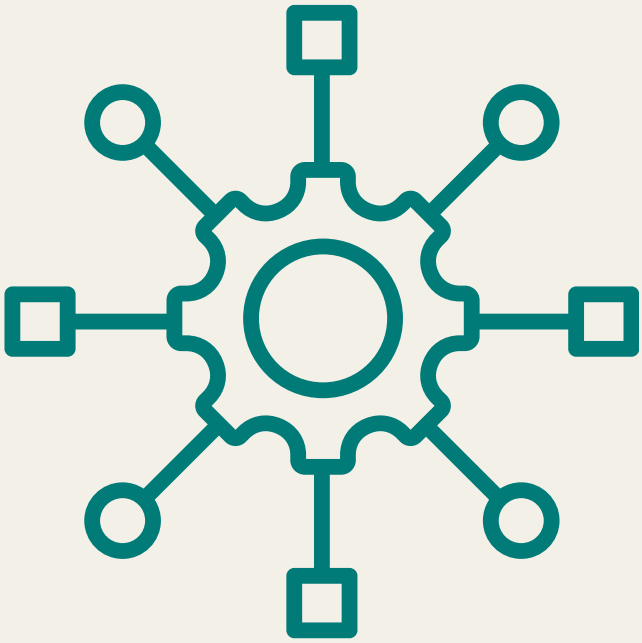
Symmetric Encryption



This diagram shows how the sender and recipient in symmetric encryption use the same key.

Symmetric encryption is efficient, but the key itself is a major vulnerability. For two people or devices to communicate through a symmetric algorithm, they must be using the same key. However, the key must remain secret -- otherwise, any interloper who gets their hands on it can read the encrypted messages. Symmetric encryption is also called **private key encryption**.

The risk of compromised keys means that one of the best use cases for symmetric encryption is protecting **data at rest**, such as proprietary databases or cloud storage folders. If only one party is involved in the transaction, there's little risk of the key leaking. However, symmetric encryption can be used to communicate securely when paired with asymmetric encryption.



Asymmetric Encryption

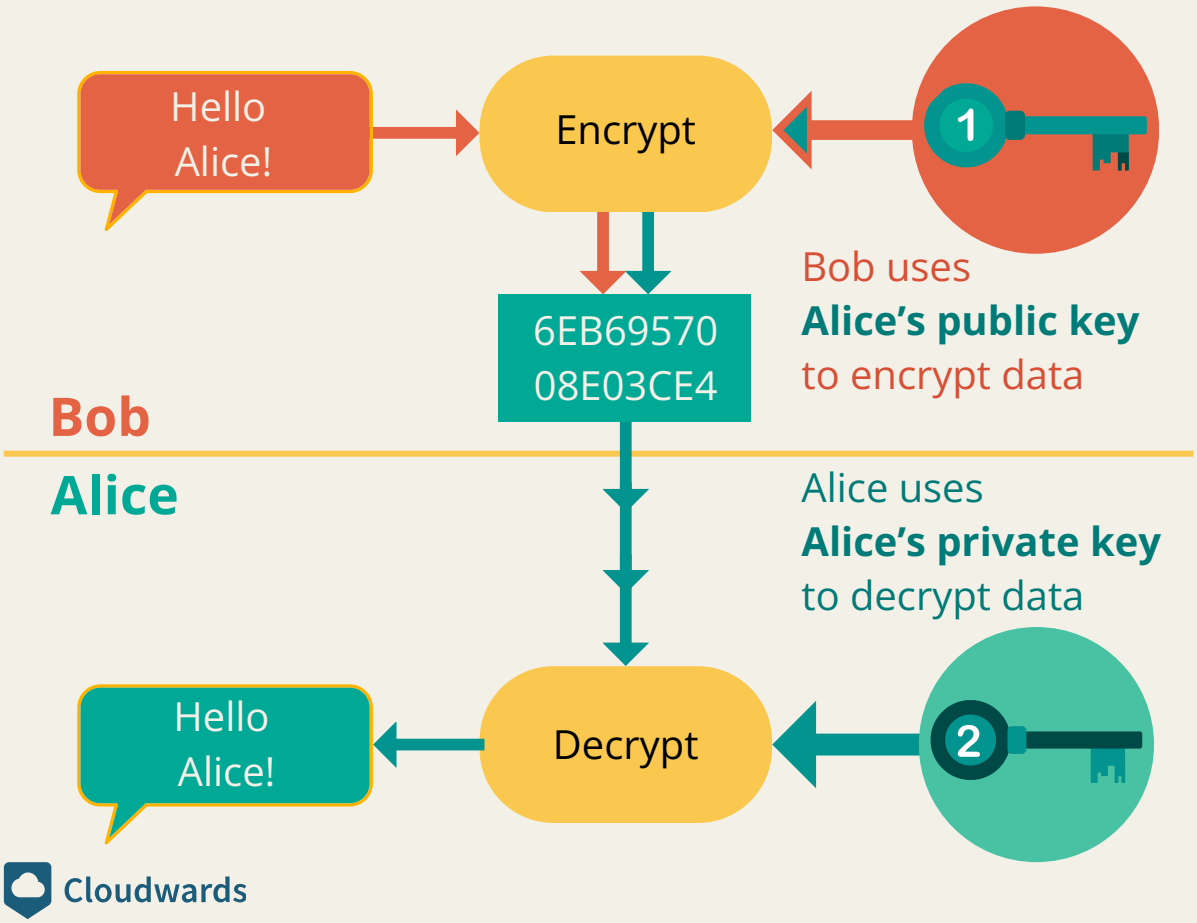
In asymmetric encryption, **the sender and recipient use different keys to encrypt and decrypt the plaintext. Each participant has:**

- a **private key** that only their device knows and a
- **public key** that is made available to anyone.

The keys are mathematically related, which allows one key to encrypt the data and the other key to decrypt the data, though they are not the same key.

When the sender wants to transmit data to the receiver, the sender will use the receiver's public key to encrypt the data, then the receiver will decrypt it with their own private key.

Asymmetric Encryption



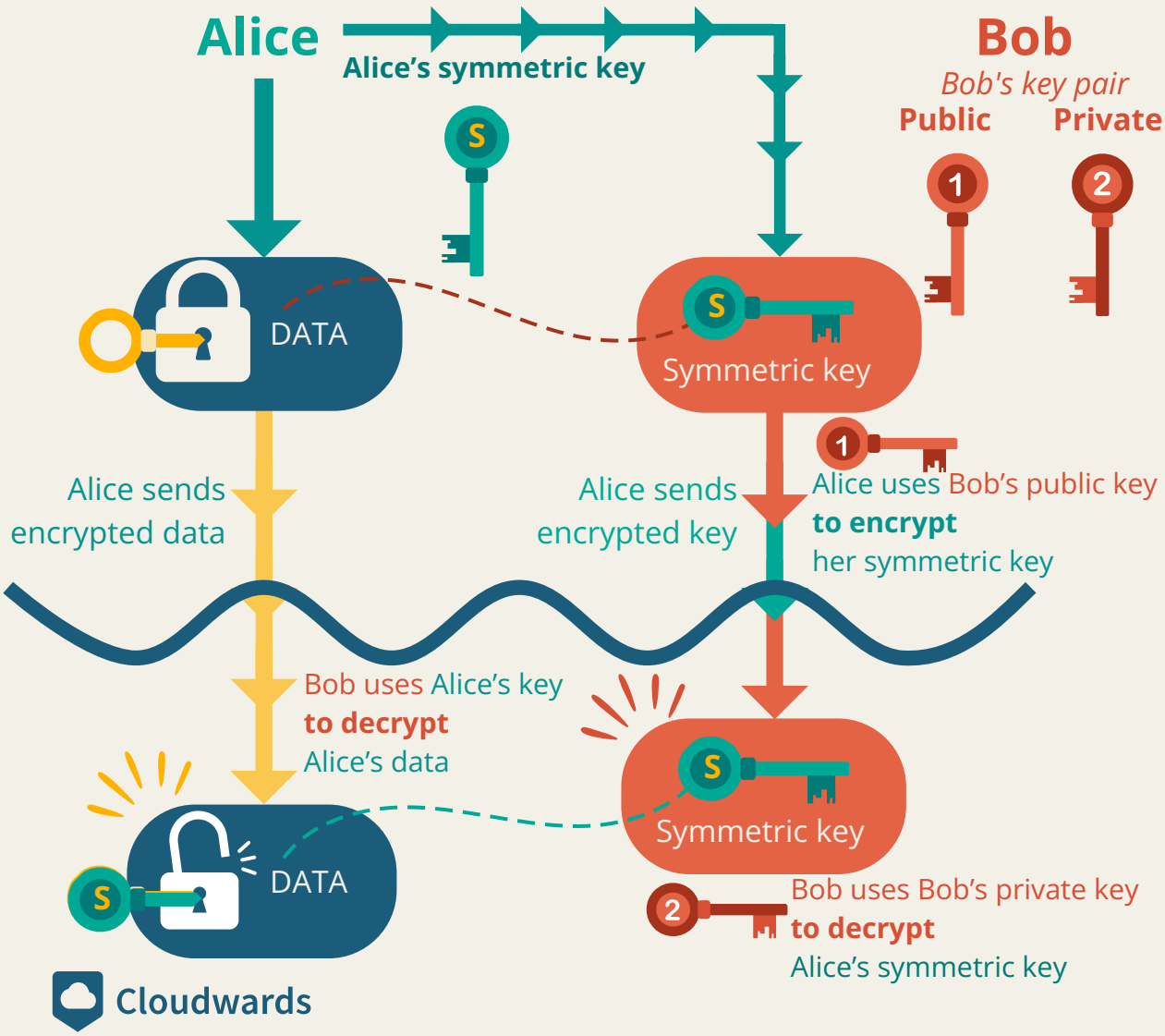
This diagram shows how the sender and recipient use the receiver's key pair, utilizing two different keys to encrypt and decrypt the plaintext.

Key Exchange

The above is a simplified version of what is normally done in asymmetric encryption. You can also use asymmetric encryption to exchange symmetric keys. Let's say a sender, Alice, wants to transmit a sensitive document to a recipient, Bob. Alice uses a **symmetric algorithm** to encrypt the document, but Bob doesn't have the symmetric key.

To send the symmetric key securely, **Alice encrypts the symmetric key with Bob's public key**. Anyone can send Bob an encrypted message using this public key, but only Bob has the right **private key** to decrypt it.

Key Exchange



In a key exchange, a sender uses the recipient's public key to encrypt the symmetric algorithm. The recipient then decrypts the algorithm with the private key.

This secure key transmission is known as **key exchange**. Once Bob receives Alice's message, he'll have the symmetric key he needs to decrypt Alice's original document. Thanks to asymmetric encryption, Alice and Bob managed to transmit a symmetric key in plain sight without any risk of compromise.

The reason why Alice doesn't use asymmetric encryption for the entire sensitive document is that **symmetric encryption is easier** because it is based on simpler math. Large amounts of data transmit much faster in a symmetric exchange. Using asymmetric encryption to guarantee the security of symmetric encryption is the best of both worlds.

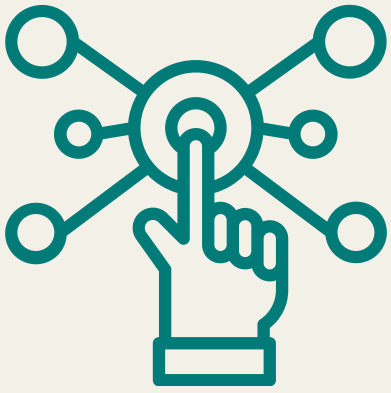
For a long time, the asymmetric encryption algorithm most frequently used for key exchange was **RSA**, but use of the **Diffie-Hellman** algorithm is increasing. Diffie-Hellman generates a shared secret number for each key exchange based on a combination of public and private keys.

Applications of Encryption in Data Security

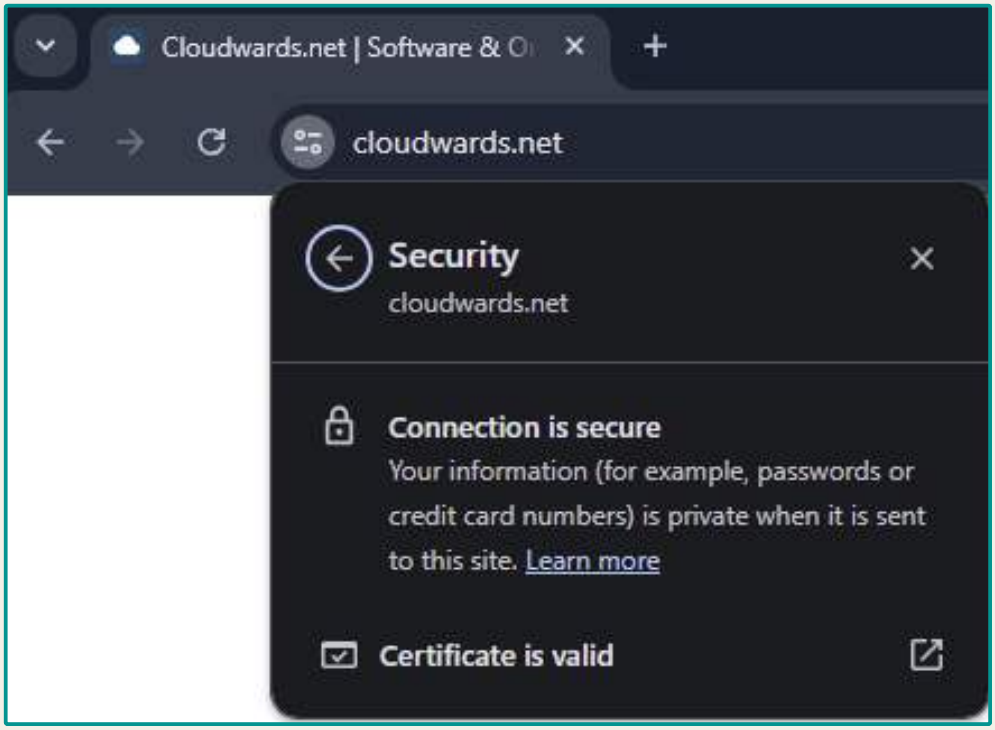
Let's recap a bit. Cybersecurity aims to protect two types of data: **data at rest**, which is stored in one secure location, and **data in transit**, which moves between two or more devices. When data is at rest, symmetric encryption is secure enough because the key never leaves its secure location.

However, data is less secure when it moves (think about how thieves in movies are always trying to steal money when it's being moved between banks). We use asymmetric encryption for data in transit to protect symmetric keys from cybercriminals.

Asymmetric encryption is also useful for **authentication**, the process of confirming a message sender's identity. One device can add a **digital signature** to a message that relies on its unique private key. If the other device can't decrypt the signature with the sender's public key, the document may have been tampered with, or another device may have taken the sender's place.



The **Transport Layer Security (TLS)** communication protocol manages authentication and encryption. Organizations called certificate authorities issue **TLS certificates** that authenticate servers hosting websites. A TLS certificate confirms a server's identity and shares its public key, acting as a trusted starting point for devices to share encrypted communication with the server.



You can click the padlock on your URL bar to see which authority verified the certificates for the site you're on.

If you've been using the web for a while, you may have noticed that the "http" in URLs now almost always reads "https." HTTPS simply means that an HTTP website is communicating via TLS -- in other words, it's encrypted. The widespread adoption of HTTPS has made the internet significantly safer overall, but there's more work to be done.

Chapter 3: Encryption in Everyday Life

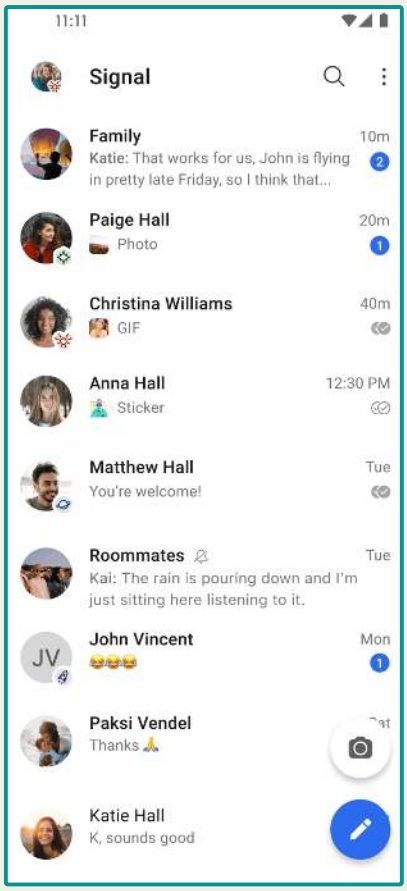
Nothing we talked about in Chapter 2 is theoretical. You may not realize it, but encryption is relevant to almost every digital interaction. The vast majority of websites now secure their information using TLS; if you use the internet at any point during your day, you're using this technology.

Thanks to TLS and HTTPS, it's almost impossible for an interloper to see what you do on a website (though your browsing activity itself is still unencrypted -- see Chapter 5 for more details on protecting it with a VPN). In this chapter, you'll learn about some of the other ways encryption technology applies to your everyday life.

Messaging Apps

Today, almost any software you use to send text messages features **end-to-end encryption**. This is not an algorithm; it's a general design philosophy. "End-to-end" means the messages are encrypted on the sender's device and not decrypted until they reach the recipient's device.

Though end-to-end encryption is ubiquitous in messaging apps, it's not equal in all of them. Facebook Messenger, the most popular messaging platform in the United States, was the latest major app to enable default end-to-end encryption in March 2024.



Signal is an open-source encrypted messaging app endorsed by Edward Snowden.

Another important detail to note is that **cellular data networks are encrypted by default**. This doesn't mean they're completely invulnerable, but it does make cell data a safe alternative to sending messages via unencrypted WiFi networks.

Online Banking

End-to-end encryption is also crucial for banking, where any data breach could have massive repercussions. To understand why, remember that the internet is a relay system that bounces signals between several nodes before they reach their destinations.

Whenever you log in to your bank account, your credentials go through several intermediary servers before reaching the bank. If a hacker were to compromise or replace any of those servers, they could see your bank account information. That's why online banking websites must encrypt data before it leaves your device.

Financial institutions often rely on the 256-bit Advanced Encryption Standard (AES-256), which is often called "**bank-grade**" encryption.

Internet of Things

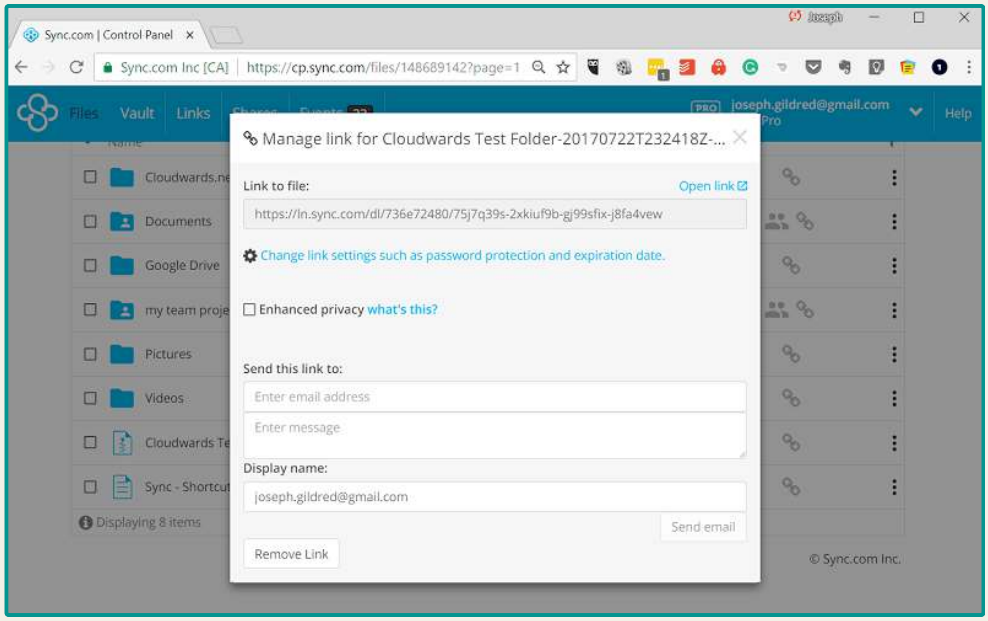
Internet of Things (IoT) devices transmit information to web servers -- a serious security risk since many of these devices are used in sensitive healthcare, home and transportation settings. Baby monitors and insulin pumps have revealed vulnerabilities. In one case, white-hat hackers showed that they could hack the systems of a moving vehicle, leading to widespread recalls.2

Since IoT is a new industry, security measures have not yet been universally adopted, though some manufacturers are taking the necessary steps. **Don’t use any IoT device that doesn’t have a documented plan for end-to-end encryption.**

Cloud Storage

Cloud storage services keep your data in a single place. Since the data is only ever encrypted and decrypted on one server, it's a bit less vulnerable. To ensure cloud security, companies tend to use AES-256 or other symmetric encryption algorithms to protect your data from anyone who doesn't have the password.

With cloud storage, a new concept enters the equation: **zero-knowledge encryption**. Different from end-to-end encryption, "zero-knowledge" means that those overseeing the encrypted files -- in this case, the cloud storage service -- do not have the keys to decrypt it. Some services are zero-knowledge by default, while others can be encrypted with third-party apps.



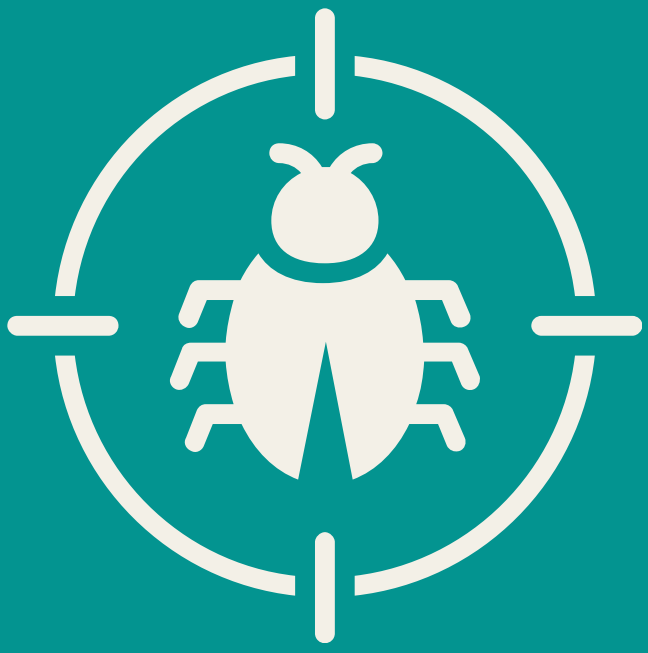
Sync.com protects its users' data with zero-knowledge encryption.

Zero-knowledge encryption removes the service as a point of failure, but it comes with the additional danger of **you being the only one holding the key**. If you lose your password to zero-knowledge cloud storage, you can never regain access to your files.

Chapter 4:
The Evolution of Cyberattacks

Like a superhero and their nemesis, security and crime evolve together. New forms of attacks spur the development of new defensive technologies, which criminals then work to overcome.

We've talked about cyber threats in general terms, but it's time to get a deeper idea of the current danger. This chapter will illustrate the changing world of cyber threats by comparing three malware milestones: the **ILOVEYOU** virus, **Stuxnet** and **WannaCry**.



ILOVEYOU

In the ’80s, network access was so rare that the **Morris Worm** -- one of the first real computer viruses -- managed to infect 10% of the entire internet in 1988.3 Barely a decade later, the internet was unrecognizable, with millions getting online through dial-up connections. As usage increased, so did the potential damage from each attack.

A man in the Philippines created the ILOVEYOU malware in 2000 to steal internet passwords to avoid paying for dial-up.3 Onel de Guzman used an early version of social engineering to spread ILOVEYOU, emailing huge batches of love letters with the malware attached. When lonely souls clicked the attachment, the malware stole their passwords and often caused additional damage.

De Guzman was arrested after ILOVEYOU briefly paralyzed the United Kingdom’s parliament.4 However, in a fascinating coda, he had to be released because the Philippines didn’t have any cybercrime laws at the time.

Stuxnet

In the 2000s, everything had changed. Cyber threats had grown to the point of changing the course of wars. **Stuxnet**, developed by the United States and Israeli governments, is considered to be the first nation-level cyber weapon. U.S. presidents George W. Bush and Barack Obama approved the development of Stuxnet, though neither administration directly acknowledged it.5

The goal of Stuxnet was to shut down Iran's nuclear weapons program as an alternative to ground invasion. Stuxnet used a complex series of exploits that enabled it to take over a nuclear centrifuge, causing the highly delicate machines to break down during the uranium refinement process.

Iran's nuclear weapons facility was **air-gapped**, meaning it had no digital connection to any outside systems. To smuggle Stuxnet inside, intelligence agents recruited an engineer to install it in a new water pump. From there, the worm replicated as designed, destroying hundreds of expensive machines and setting the Iranian nuclear program back years.

Stuxnet had such a specific target that it was never a serious threat to the wider internet. However, it marked a turning point in cybersecurity, as it was the first time nations had used malware to advance their geopolitical interests -- a trend that would lead to far more indiscriminate attacks, potentially including the one we'll discuss next.

WannaCry

On May 12, 2017, computers all over the world running Microsoft Windows 10 began to see aggressive pop-up messages written in broken English. These messages informed them that their files were now encrypted and inaccessible, and that the only way to decrypt them was to send a Bitcoin payment to a certain address.

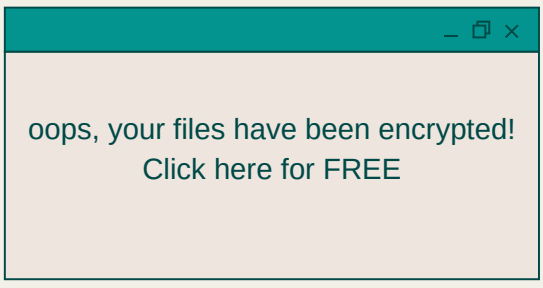
This blatant shakedown made **ransomware** a household word for the first time. It frightened a lot of people, especially since the hackers threatened to delete the files if payment wasn't sent in a timely manner (though later research showed the program wasn't actually capable of doing this). Much of today's ransomware is built on the foundation WannaCry laid.

How did it happen in the first place? Researchers believe the fault may lie on both sides of another geopolitical dispute. Symantec investigations revealed clear signs of involvement by the Lazarus Group, a hacker collective that answers to the government of North Korea.6

Meanwhile, Microsoft has accused the U.S. National Security Agency (NSA) of discovering the Windows 10 vulnerability that allowed WannaCry to spread but keeping the knowledge to itself until The Shadow Brokers, a different group of hackers, leaked it. Multiple governments worked to exploit a vulnerability for their own purposes, and the result was a devastating cyberattack.7

However, the most important lesson from WannaCry is one we can all apply. Microsoft had actually patched the vulnerability months before May 2017, but many computers still hadn't downloaded the update. **Simply updating the software in a timely manner** could have protected those systems.

Today, several governments are known to sponsor hacker groups, such as Russia, China, North Korea and Iran. The existence of nation-level cybercrime proves there are major advantages to exploiting connected systems. Someone will always try to exploit flaws for gain. If we want a usable internet, we must ensure widespread and updated encryption and cybersecurity.



Chapter 5: Securing Your Digital Footprint

We've talked a lot about cybersecurity at this point. You know which threats people and organizations face online, how they respond to those threats and how that technology makes its way into your everyday life. We also shared a few tips at the end of Chapter 1 on what you can do to keep yourself safe.

This chapter will **expand on those tips** and give you more tools for shoring up your own cybersecurity. If you apply this advice, hackers will have very few opportunities to mess with you -- even ones with government-backed resources.

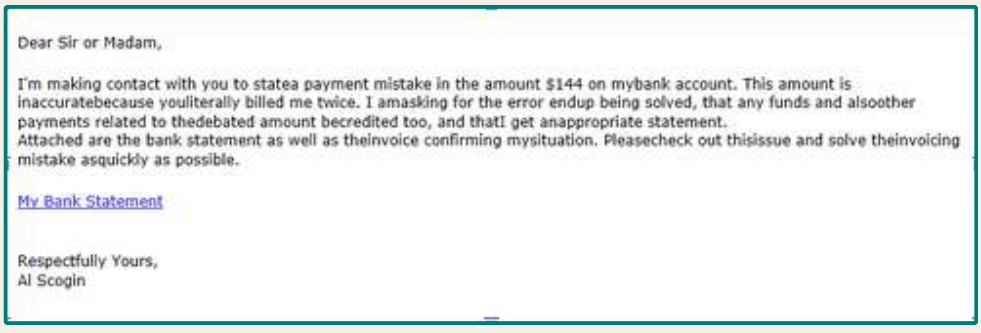
Don’t Open Suspicious Emails

Since the ILOVEYOU virus first spread a quarter-century ago, email has been a popular and successful way to sneak malware onto unsuspecting devices. Even Onel de Guzman’s **social engineering** methods are still effective today.

Phishing attackers use the following tactics to make you click on a link or open an attachment containing malware, or to make you hand over data on your own:

- Impersonating institutions like banks, credit bureaus or government agencies
- Instilling a sense of panic through dire warnings and red letters
- Claiming that you must act to solve vague yet urgent problems
- Using personal details about you to appear legitimate (sometimes called “**spear-phishing**”)
- Creating fake versions of legitimate websites or emails

Being aware of these tactics robs them of their power. Whenever you see a scary email, take a deep breath and double-check the source. Does the email match the name of the institution claiming to have sent it? Does the website match the institution’s URL? Does the email make any specific claims or simply use vague but frightening language?



Dear Sir or Madam,

I'm making contact with you to statea payment mistake in the amount $144 on mybank account. This amount is inaccuratebecause youliterally billed me twice. I amasking for the error endup being solved, that any funds and alsoother payments related to thedebated amount becredited too, and thatI get anappropriate statement.
Attached are the bank statement as well as theinvoice confirming mysituation. Pleasecheck out thisissue and solve theinvoicing mistake asquickly as possible.

My Bank Statement

Respectfully Yours,
Al Scogin

In the age of generative AI, you’re unlikely to find a phishing email this poorly written. Instead, learn to verify based on the clues listed above.

If you’re ever unsure, you can always contact the institution yourself and ask whether they sent the email. Above all else, the first rule of email security is to **never open a link or attachment if you can’t confirm who sent it**, even “unsubscribe” links.

Be Careful With What You Share

As we mentioned above, attackers can take the personal details you post publicly on social media and use them to make scams appear legitimate. These details can also be used to guess weak passwords.

Protecting your online privacy depends largely on the kind of information you share online. Don't be too quick to share sensitive details about yourself, especially your email address, location and other personally identifiable information. If a website requires your email address to access its content, you can **use a temporary throwaway email instead**.

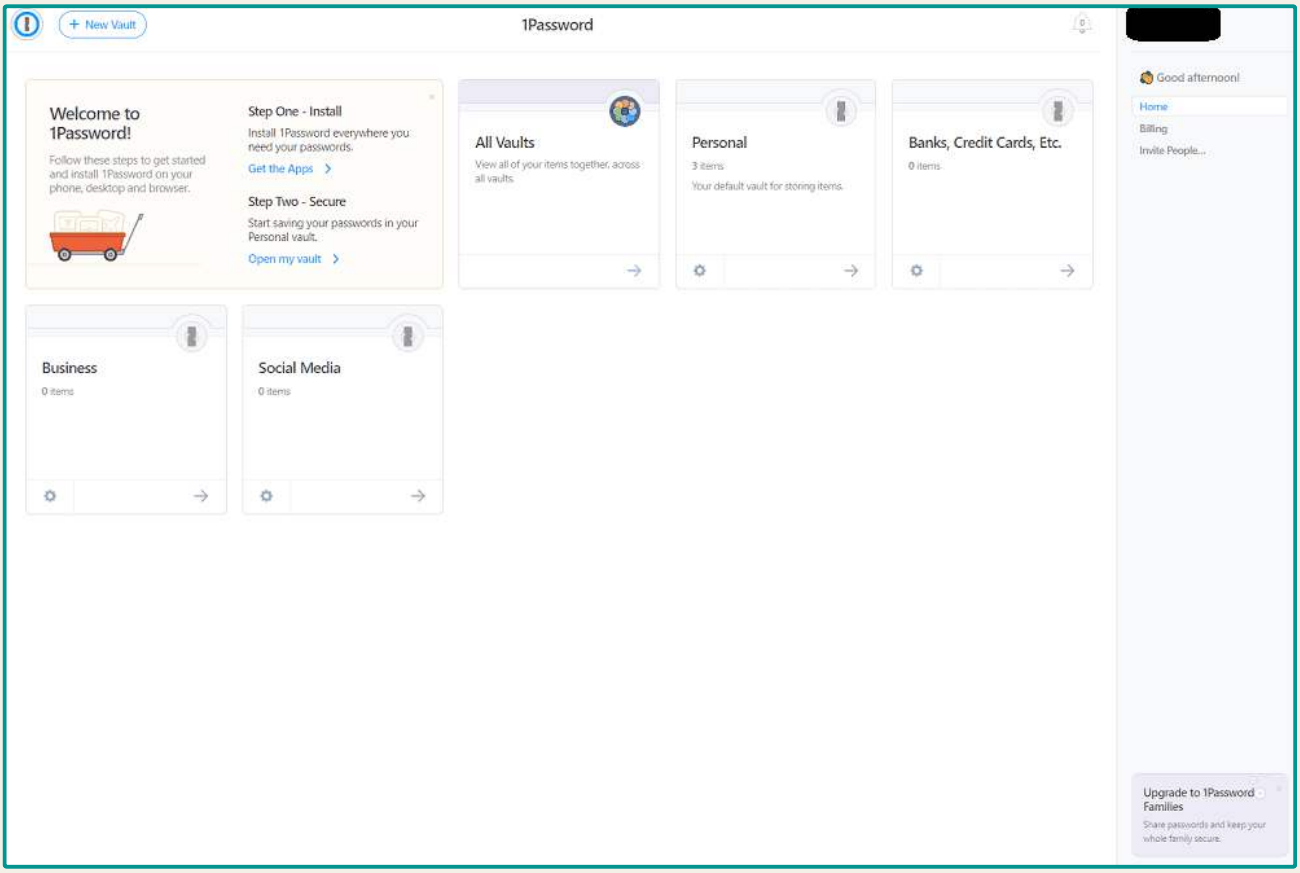
This doesn't mean you have to give up on social media altogether, but we do recommend **changing your privacy settings** so only your trusted friends can see what you post.

Download and Apply Every Update

Devices that haven't been updated in a while are prime targets for malicious actors. **Updates often include security patches and bug fixes**, such as those that would have prevented WannaCry. We recommend setting your device to update automatically.

Use a Password Manager

Verizon's Data Breach Investigations Report (DBIR) shows that 80% of data breaches occur due to stolen, weak or compromised passwords.1 However, creating robust passwords isn't always easy -- they must be complex yet memorable. A **password manager** is the perfect solution because it generates passwords that are nearly impossible for intruders to guess.



Password managers like 1Password remove all the obstacles that make password security a hassle.

Moreover, **password managers save your passwords so you don't have to remember them.** Many also automatically fill in your password when you click the icon on a login page.

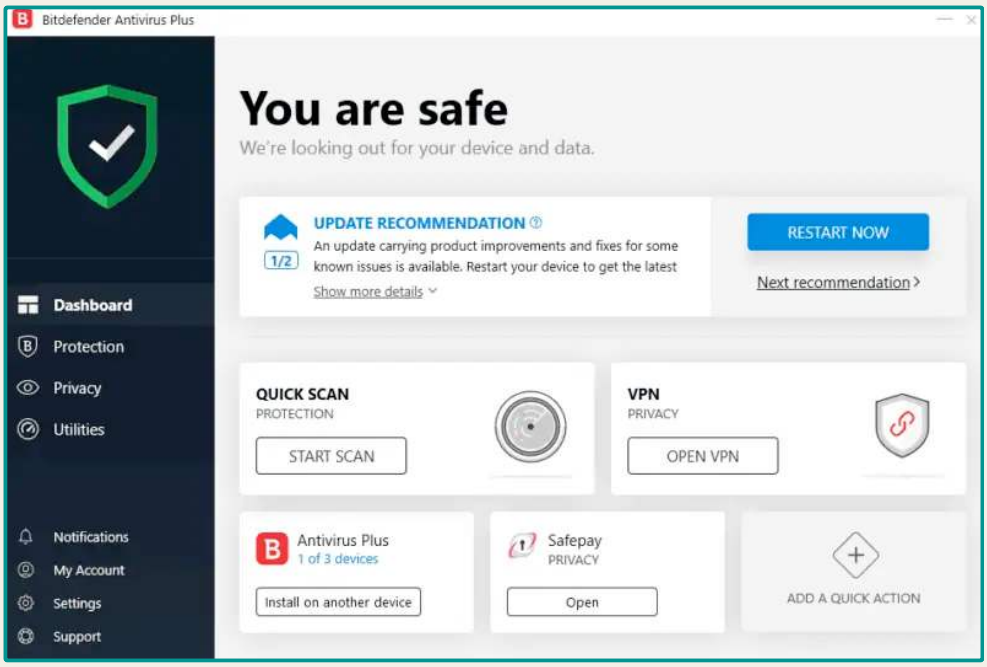
Use Two-Factor Authentication (2FA)

Two-factor authentication adds an extra level of security to your online accounts that can blunt the impact of a compromised password. Whenever you log in to a website, instead of using a single factor like your password, you'll use two factors, like your password and a single-use code sent to your email.

As long as you have 2FA enabled on your online account, attackers won't be able to access that account, even if they have your password. Of course, this does require that **you use different passwords for each account**.

Run Regular Virus Scans

Every day, thousands of malicious software programs are introduced on the internet. The AV-TEST Institute registers more than 450,000 malicious programs and potentially unwanted applications (PUAs) daily.



Bitdefender Antivirus can run multiple types of scans to catch malware on your device.

An antivirus program can detect and remove such files. Moreover, it can do so at any point in the process, from intercepting the malware before you download it to purging it once it's already active on your system. You can set the program to regularly scan your entire system in the background, catching malware no matter how it reached your device.

Use a Virtual Private Network (VPN)

A VPN makes your internet activity far more secure than relying on HTTPS alone. These apps create an encrypted “tunnel” between your device and the internet, changing your IP address (a unique online identifier) to an innocuous one the VPN itself owns. With a VPN active, neither your ISP nor anyone else can see who you are, where you are or what you’re doing online.

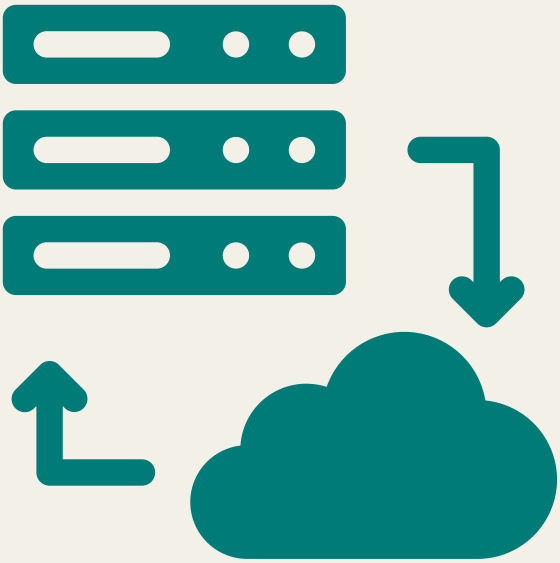
What Are the Best VPNs?

1. Best VPN Overall	2. Best Budget VPN	3. Best VPN for Beginners
NordVPN	Surfshark®	ExpressVPN
Best Value plan: **Basic** **30-Day Refund Period**	Best Value plan: **Starter** **30-Day Refund Period**	Best Value plan: **Annual** **30-Day Refund Period**

Back Up Your Data

If your phone or computer is compromised, a factory reset could be the only way to remove all malicious code. However, you may lose all your data in the process. Back up your data to the cloud so you can retrieve it in the event of an emergency.

A good backup also makes ransomware a lot less scary. If hackers forcibly encrypt your files, you won't have to pay them a dime -- you can just retrieve the data from your backup.



Chapter 6: Cybersecurity in the Workplace

The previous chapter covered personal cybersecurity. In this chapter, we'll switch gears and discuss the demands of securing an entire office. This information is still relevant even if you're not directly involved in information technology (IT) -- IT departments can function much better when the rest of the workplace understands what they're doing and why.

As you learned in Chapter 4, this era is characterized by cyberattacks like WannaCry that primarily target large organizations. The reason is simple. Not only do businesses and institutions have more money than individuals, but they also have **many more points of failure**. One employee using a weak default password can compromise an entire billion-dollar company.

Workplace cybersecurity is a combination of regular technical updates, employee training, crisis planning and legal compliance. We'll explore how each of these pertains to your office life.

The Role of IT Professionals

Your IT department is more than just the people you call when your internet isn't working. IT professionals are also responsible for making sure business networks are secure. This involves tackling a wide range of jobs, including:

- **Access controls**: Not everyone who works in an office has access to all of that office's data. When leaders make decisions about who should have access to certain data, IT is responsible for applying those decisions. This ensures that one hacked computer doesn't impact the entire workplace network.
- **Network monitoring:** IT representatives keep tabs on all connected devices in the office to look for suspicious activity. A modern department will use a combination of hardware and software to monitor the office network from a centralized dashboard.
- **Endpoint detection:** IT professionals know that "endpoints" -- a catch-all term for user devices on the network, including desktops, laptops and phones -- present the most vulnerable targets on a network. Many use some variety of endpoint detection and response (EDR) software to watch for hacks originating on personal computers.
- **Software updates:** IT is responsible for making sure all software in the office is swiftly patched and updated when necessary. Some have adopted tools that handle this process automatically.
- **Vulnerability scanning:** IT departments audit systems in the hopes of catching potential exploits before hackers do. This entails keeping a careful inventory of all digital resources and regularly checking them on a database of known issues.

If you're not in the IT department, the best way to help is to **immediately download all available software updates**. This ensures your computer has the best possible protection, even if IT isn't actively watching it.

Employee Training Programs

Training is perhaps the most critical ingredient in a workplace cybersecurity plan. Any employee can pose a risk if their device is compromised, which means **every employee is part of the solution**. IT staff and HR training professionals work together to make sure everybody in the office knows how their actions impact overall cybersecurity.

The lessons they teach will likely be non-technical, instead focusing on basic threat recognition skills. Potential trainings include the following:

- **Recognizing phishing and social engineering:** Employees should know how to distinguish legitimate emails from phishing attempts, and know how to recognize the telltale signs of social engineering, including vague threats, spoofed email addresses and demands for immediate action.
- **Using strong passwords:** The best workplace password policy is for employees to use passwords that are long yet memorable, unique on each device and changed regularly.
- **Understanding physical security:** It's important to grasp how physical security and cybersecurity interact. If a hacker penetrates the office's physical security, they unlock many more avenues for compromising cybersecurity. Employees can help by being aware of all workplace security protocols.

A physical security failure can threaten cybersecurity in ways you may not expect. Hackers can steal devices to unlock later or launch **real-world phishing attacks.** In one case, a hacker disguised as an employee entered an office and posted their phone number on a bulletin board as the "new IT helpline." They collected several employees' usernames and passwords.

Incident Response Protocols

Even well-monitored networks can be breached from time to time. Every office should have an incident response plan (IRP) in place in case cybersecurity fails. At a minimum, an IRP should include:

- Contact information for relevant law enforcement, including local police and the FBI
- Instructions on who to notify in the event of an incident
- A clear plan detailing which employees will play which roles in the response, including an **incident manager** to coordinate, a technical expert and a communications expert
- Pre-drafted press releases
- Relationships with outside vendors who will play a role, including security firms, legal counsel and insurance companies

It can be valuable to **rehearse your incident response** at least once per quarter by playing through a simulated scenario.

Data Security Compliance

One final duty for IT departments is to ensure compliance with the law by storing all data according to national regulations. IT departments should consult with the legal department to keep up with federal laws, especially those that apply directly to the organization's industry. We'll discuss some of these regulations in the following chapter.

Chapter 7: International Cybersecurity Regulations

The Philippines wasn't alone in its lack of laws to regulate cybersecurity or prosecute offenders in 2000. Governments as a whole have been slow to catch up with the pace of technological change, with even the United States lacking a comprehensive data protection law (though several states have their own regulations).

However, the legal landscape is evolving worldwide. In this section, we'll explain the importance of two regulations and their relevance to cybersecurity: the **General Data Protection Regulation (GDPR)** in the European Union and the **CyberSecurity Information Sharing Act (CISA)** in the United States.

General Data Protection Regulation (GDPR)

The GDPR is a data privacy law that protects EU citizens' personal information. Adopted in 2016, it came into force on May 25, 2018, and it applies to any company that processes personal data belonging to EU citizens, regardless of where the company is located.

The GDPR grants EU citizens several important rights. It stipulates that a company cannot process a user's personal data without gaining explicit consent from the user. It also lets the user view and correct any personal data relating to them.

Importantly, the GDPR includes the so-called **right to be forgotten**, which means that a user can choose to have all their data deleted, and the company must abide by that choice. It also stipulates that if a company suffers a data breach, it must inform all affected users. Each company must also employ a data protection officer (DPO) to handle all GDPR-related issues.

One of the seven principles of GDPR is **integrity and confidentiality**: Personal data must be secured in a way that protects it from theft, accidental loss or unauthorized processing. That means any company that manages data must ensure it is encrypted and backed up.

In effect, the **GDPR makes businesses liable if your data is compromised in a breach.** Several Fortune 500 companies have already been fined on the basis of this regulation, including Facebook's parent company Meta, Marriott Hotels, British Airways and TikTok.

Cybersecurity Information Sharing Act (CISA)

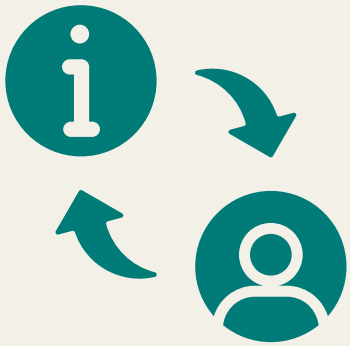
The Cybersecurity Information Sharing Act (CISA) should not be confused with the Cybersecurity and Infrastructure Security Agency, which shares the same acronym. U.S. president Barack Obama signed the CISA legal regulation into law in 2015.

CISA aims **to make it easier for U.S.-based corporations to share data with the Department of Homeland Security (DHS)** so it can counter cyber threats. Companies aren't required to share information but are safe from legal liability if they do. CISA requires the DHS to share relevant information with other government agencies and any affected businesses.

Proponents of CISA argued that legal barriers to information exchange had previously prevented companies from sharing information that could have foiled cyberattacks. However, CISA also had opponents, who cited fears that the DHS could use its overly broad provisions to gather information about U.S. citizens without a warrant.

CISA contains provisions requiring reports to be anonymized and preventing the exchange of protected data like health and financial information. Beyond privacy concerns, the greater issue after nearly 10 years in force is that **CISA has not definitively proven to be effective against** cyber threats. Many of the shared threat indicators have been inaccurate or unusable.

All in all, CISA is an important first step toward a nationwide security strategy, but the United States must continually update its strategy as threats continue to evolve (*see Chapter 9*).



Chapter 8: Ethical Hacking and Penetration Testing

If you've ever seen the heist film 'Sneakers,' you may remember that Robert Redford's character makes his living in an unusual way: Banks hire his team and him to rob their vaults and provide a full report on how they did it. Though it may seem odd for a company to hire its own burglars, the process illustrated in the movie has analogues to a vital cybersecurity tool.

Penetration testing is the process of discovering vulnerabilities in a system by attempting to hack it. Testers study a system, deduce potential attacks and then build countermeasures to those attacks before hackers can try them. The reasoning is that if someone discovers a flaw in your security, it should be a person or group with your interests at heart.

Penetration testing is also called **ethical hacking** or **white-hat hacking**. The latter term derives from old Western films in which heroic characters wore white hats and villains wore black ones. This view sorts hackers into three groups:

- **White hats** perform penetration testing on systems with the full knowledge and consent of those systems' owners. They may also perform general research on potential exploits and cyber threats in order to warn the community. In the latter context, you may see them called **security researchers**.
- **Grey hats** occupy a more ambiguous space. They often run penetration tests, but unlike white hats, they may do so without permission. Their aim may be to raise awareness of a critical vulnerability, to get paid for finding the problem or to show off their own skills.
- **Black hats** penetrate systems for their own personal gain, on behalf of a nation-state or, more rarely, for the sake of sowing chaos.

Despite being on the right side of the law, white-hat hackers use the same techniques as cybercriminals. They may send phishing messages, steal passwords, hijack web exchanges and install malware. Their mission is to test any possible avenue of attack without holding back.

The Penetration Testing Process

There are different ways to conduct a vulnerability assessment on a website or an application. One approach is to probe for vulnerabilities the same way a hacker would, with no inside knowledge or help. That is called **black-box testing**. The black box approach is more like what a criminal would do.

White-box testing, on the other hand, involves testing security while having access to information such as the source code of the application being probed or details about the software being used.

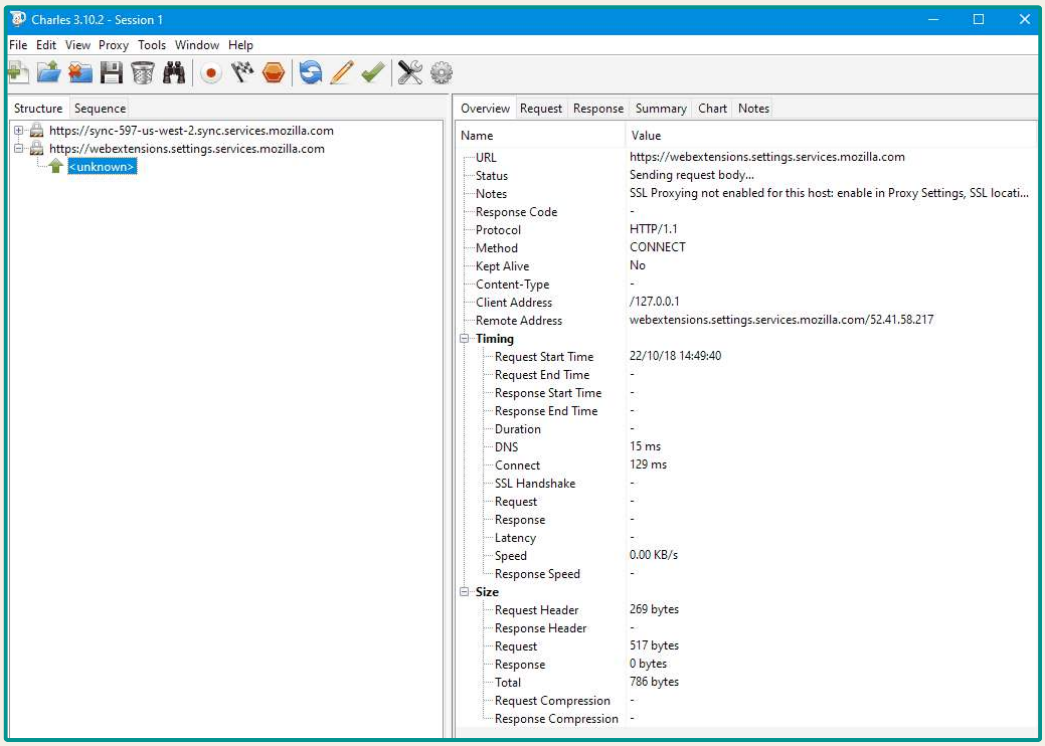
The white-box strategy makes it easier to find vulnerabilities because the tester can browse through everything and see how it all fits together. If they know which software is running, they can target their attacks accordingly. However, it may not indicate the vulnerabilities a real hacker would be likely to find.

Regardless of which strategy they choose, penetration testers generally follow a simple four-step process.

1. **Reconnaissance:** The tester gathers as much information as they can about the target system, relying on a combination of publicly available data, volunteered information (in the white-box approach) and data gleaned from interacting with the system.
2. **Vulnerability assessment:** The tester analyzes the information gathered in the first phase and notes where the system appears vulnerable. For this phase, they may draw on vulnerability databases maintained by the U.S. government.
3. **Exploitation:** The tester formulates and executes an attack strategy against the vulnerabilities identified in step two. Ethical hackers try not to crash the system while hacking it, but sometimes it's unavoidable.
4. **Reporting:** The tester informs the system administrators of which attacks worked, which were repelled and what improvements can be made.

Vulnerability Assessment Tools

Linux is a popular operating system for those involved in security testing. Kali Linux is a particularly good distribution -- it comes installed with all sorts of software, including Wireshark and the Burp suite, which can give you a detailed picture of what's going on when you connect to a website.



Charles is a tool that Linux experts can use to monitor web traffic.

Ethical hackers can use these tools to modify web requests and see how a server responds to non-standard traffic that might come from a hacker. There are also tools that automate **brute-force password attacks** by trying as many combinations as possible. Brute-force attacks are the reason why **short passwords are risky regardless of the password itself**.

Password forms are also a risk for SQL injection -- an attack that sneaks code into the data passed to the server. A security tester can spot places where injections could occur and can update the code to ensure incoming data is handled safely.

Looking into how an application uses computer memory can also reveal vulnerabilities. Testers can poke through the innards of an executable program with the GNU debugger, or GDB. This kind of vulnerability testing involves looking for exploits that might grant a hacker access to a server and the capability to take control of it.

Most browsers have a dev console, which is useful for examining what is happening on a website. Chrome's dev tools show the elements that a page loads and reveal errors. In addition to causing problems for users, errors could leave a website vulnerable to attack.

You can find the dev console in Chrome by **clicking the three dots** at the top right to open the menu and selecting **"more tools" > "developer tools."** Click the **"console" tab** to view the errors on the website you are looking at. You may be surprised to learn how much goes wrong, even on high-profile websites.

Chapter 9: Emerging Trends in Cybersecurity

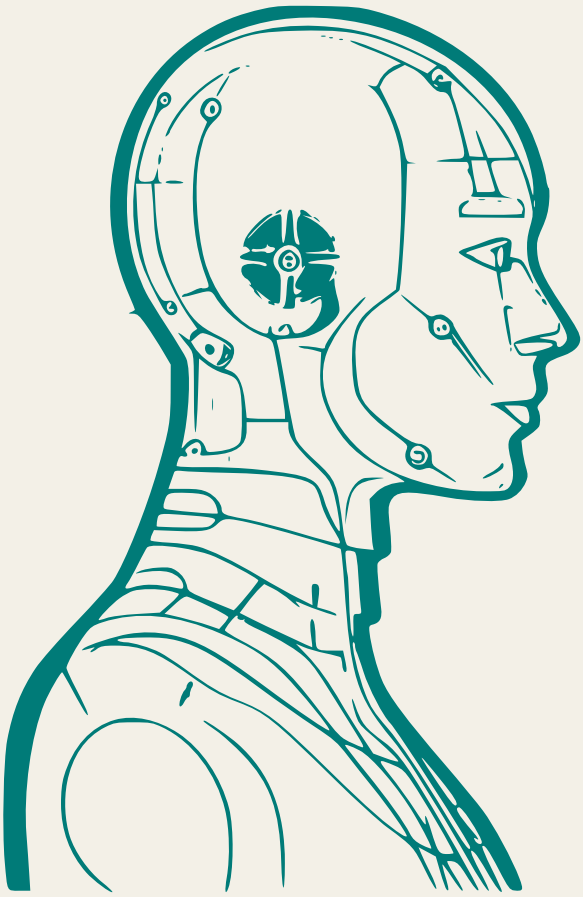
We're near the end of our course on cybersecurity and encryption. Along the way, you've learned exactly how hackers pose a threat to connected people and businesses. You've also learned the easiest ways to protect yourself and gained a sense of what professional experts do to protect large-scale systems.

However, cybersecurity is not a static field. Both hackers and security experts are constantly in search of new advantages. Furthermore, technological breakthroughs often provide new avenues to both sides of the fight. In this last chapter, we'll discuss some of the trends shaping the future of cybersecurity.

Artificial Intelligence

Generative AI is a prime example of a new development that's offered boons to both security systems and criminals. Cybercriminals are already using AI to produce extremely believable social engineering scams, even **replicating voices to make their phishing more realistic**. With AI, hackers can launch more spam in less time.

On the other hand, AI has helped security teams respond to threats more efficiently. For years, antivirus programs have used machine learning to **predict malware signatures before they're used**. Recent advances have made AI even better at processing huge amounts of data to look for vulnerabilities and criminal activity.

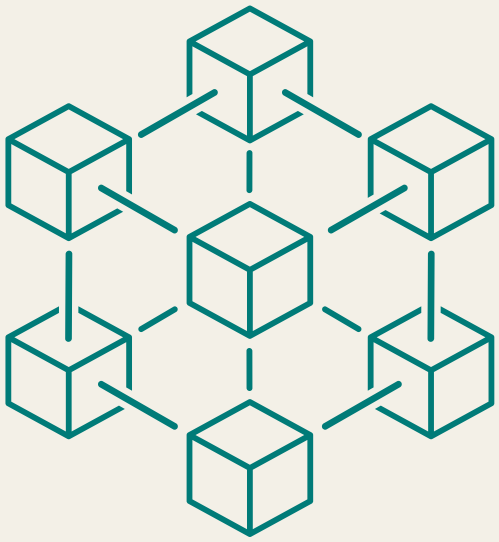


Blockchain

Blockchain technology is a tool for guaranteeing total data accuracy by distributing the data across many computers, theoretically making it **impossible for malicious actors to tamper with it**. Since much of cybersecurity relies on verification through accurate data, blockchain can be used to create trust.

Specifically, some experts argue that blockchain can be used to create a more secure public key infrastructure by protecting digital certificates against subversion (see Chapter 2). Blockchain eliminates the need for a trusted certificate authority to verify a server's identity, as **the same authentication can be completed through group consensus.**

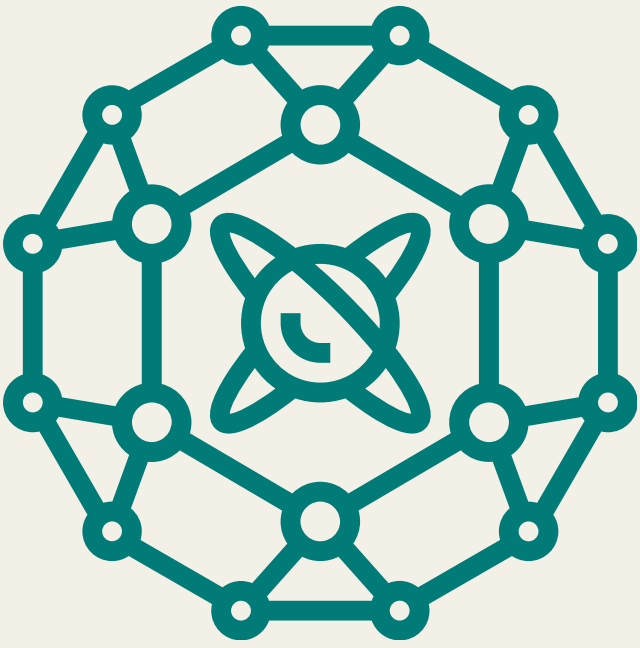
However, substituting blockchain for existing authentication methods has obstacles. Migrating can be prohibitively expensive for smaller businesses, and the ledger's universal accessibility raises data privacy concerns. It remains to be seen how widely blockchain will be adopted as a security tool.



Quantum Cryptography

Quantum computing technology has yet to become widely viable, but it could allow computers to process data much faster than they can today. A quantum computer can hold binary bits in both the 0 and 1 states simultaneously and thereby run many calculations in parallel.

If the tech ever matures, it could pose a danger to our current best encryption algorithms. AES-256, which would normally take billions of years to crack, could fall to a quantum brute-force attack. In that case, our only recourse would be quantum encryption created by the same quantum computers. Just like with AI, the technology is its own antithesis.



Biometric Authentication

Biometric authentication is already a widely used technology -- if you've ever unlocked your phone with your fingerprint, you've participated in biometric cybersecurity. Biometrics relies on the **unique, irreproducible nature of bodily traits** to verify a user's identity. Examples include retinal scans, fingerprint scans, voice pattern analysis and facial recognition.

However, as spoofing technology grows more sophisticated, it may be possible for cybercriminals to replicate a biometric signature. Biometric data also creates privacy concerns, as it requires intimate information that would violate users' rights if not stored properly.

The best current solution to protect against compromised biometric traits is **multi-factor authentication**, which we discussed in Chapter 5. When combined with a password and a physical token, biometric locks are much harder to subvert.

Conclusion: The Future of Cybersecurity

If there's anything security researchers are good at, it's thinking ahead. Case in point: The first paper to mention that quantum computers might threaten traditional cryptography was published back in 1994. Hackers may be creative and motivated, but the people fighting them are, too.

If computer security interests you, it has never been easier to get involved. More companies than ever offer public bounties for those who find and report issues with their websites. Prizes can reach as high as hundreds of thousands of dollars, though most are much lower.

That said, bag a few small prizes and you might be able to land a job as a security consultant or penetration tester and teach companies how to protect themselves from the less scrupulous bug hunters out there.

Author - Sam Chapman

Snap Shot
Samuel Chapman is a writer and editor for Cloudwards. His writing and research focus on VPNs, anonymity and online privacy.

Background & Education
Samuel Chapman is a writer and editor at Cloudwards and an expert in online security, privacy and cryptocurrency. His tenure at Cloudwards spans over four years, and he has also written for brands like Koalafi, Ivee and Lunchables, and serves as content manager for PrivacyJournal. Samuel enjoys delivering clear, compelling narratives that demystify complex topics for a broad audience.

As an editor, he uses his keen eye for detail and commitment to high-quality writing to make Cloudwards the best online source for understanding cloud-based technology. Outside of his professional pursuits, Samuel's passions include writing fiction, historical fencing, board games, and hiking.

Samuel holds a Bachelor of Arts in Environmental Studies from Whitman College and a Master of Fine Arts in Creative Writing from the University of Southern Maine.

Sources

1. Verizon - Analyzing the COVID-19 Data Breach Landscape
2. Wired - Hackers Remotely Kill a Jeep on the Highway—With Me in It
3. IBM - Malware History
4. The Guardian - Love Bug Shuts Down Computers
5. Reuters - Researchers say Stuxnet was deployed against Iran in 2007
6. CSO - Wannacry Explained
7. Microsoft Blog - The need for urgent collective action to keep people safe online
8. AV Test - Malware Scans

Chapter 1

- Online Privacy Guide - Cloudwards
- Data Privacy Statistics - Cloudwards
- Cyber Security Statistics - Cloudwards
- Best Password Manager - Cloudwards
- Know the Types of Cyber Threats - Mass.gov

Chapter 2

- Description of Encryption - Cloudwards
- What is AES? - Cloudwards
- What is WireGuard? - Cloudwards
- SSL vs TLS - Cloudwards
- Symmetric Key Encryption: Why, Where, and How It's Used in Banking - Cryptomathic
- What is Asymmetric Encryption? - Cloudflare

Chapter 3

- Cloud Security - Cloudwards
- Best Zero-Knowledge Cloud Services - Cloudwards
- How to Encrypt Text Messages - Cloudwards
- Best Encrypted Cloud Storage - Cloudwards

Chapter 4

- Malware History - IBM
- Stuxnet Explained: The First Known Cyberweapon - CSO Online
- Dutch Engineer Used Water Pump to Get Billion-Dollar Stuxnet Malware into Iranian Nuclear Facility: Report - SecurityWeek
- WannaCry Explained: A Perfect Ransomware Storm - CSO Online
- Nation-State Cyber Actors - CISA

Chapter 5

- What is Two-Factor Authentication? - Cloudwards
- What is Phishing? - Cloudwards
- Email Security - Cloudwards
- Ransomware Protection - Cloudwards

Chapter 6

- IT Security Professionals: Key Roles and Responsibilities - Simplilearn
- Ways to Monitor Network Traffic - Teramind
- What is Vulnerability Scanning? - Balbix
- Workplace Cybersecurity - InstituteData
- Incident Response Plan Basics - CISA

Chapter 7

- 20 Biggest GDPR Fines - Skillcast
- General Data Protection Regulation - Cloudwards
- Pros and Cons of the Cybersecurity Information Sharing Act of 2015 - ACE USA

Chapter 8

- Hacker Hat Types - Kaspersky
- Penetration Testing - Cloudwards
- Ethical Hacking in Cloud Computing - EC-Council
- Penetration Testing Phases - EC-Council

Chapter 9

- AI and Cybersecurity: A New Era - Morgan Stanley
- Cybersecurity and Blockchain - Infosys
- Quantum Cryptography - IBM
- Role of Biometrics in Cybersecurity: Threats and Solutions - Alice Biometrics

Cloudwards

Thank you for downloading our guide! We hope it's helped you on your journey to understanding cybersecurity and better protecting yourself online. If you enjoyed it, be on the lookout for other security guides from Cloudwards.