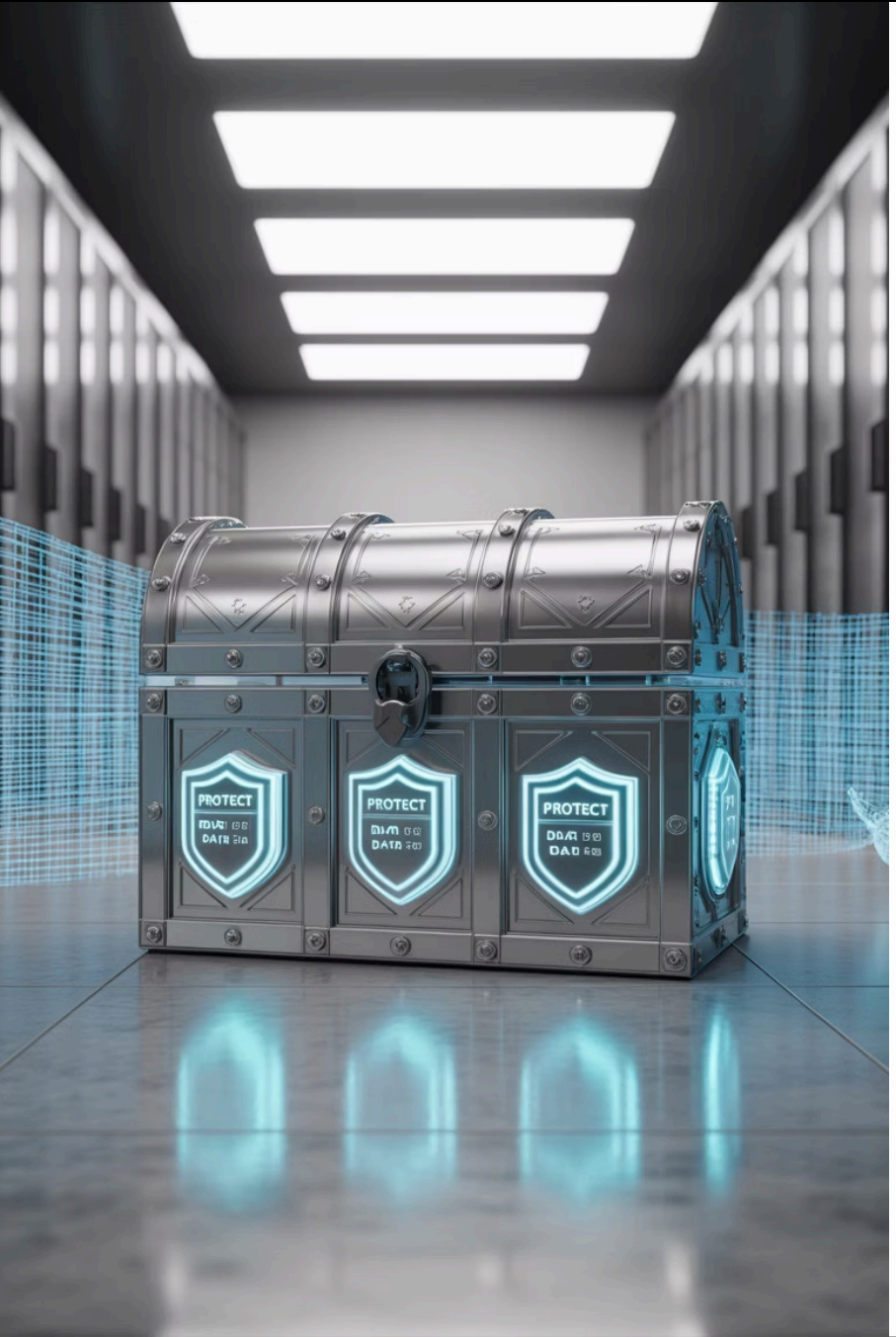



# 🔒 IT Security Rules

Imagine your digital life is a valuable treasure chest. IT security rules are the blueprint for an unbreakable lock and the code of conduct so you never lose the key or accidentally give it to a thief. These are simple but extremely effective habits that protect you from most dangers on the internet.

# 🔑 Fundamental Principles of Secure Passwords

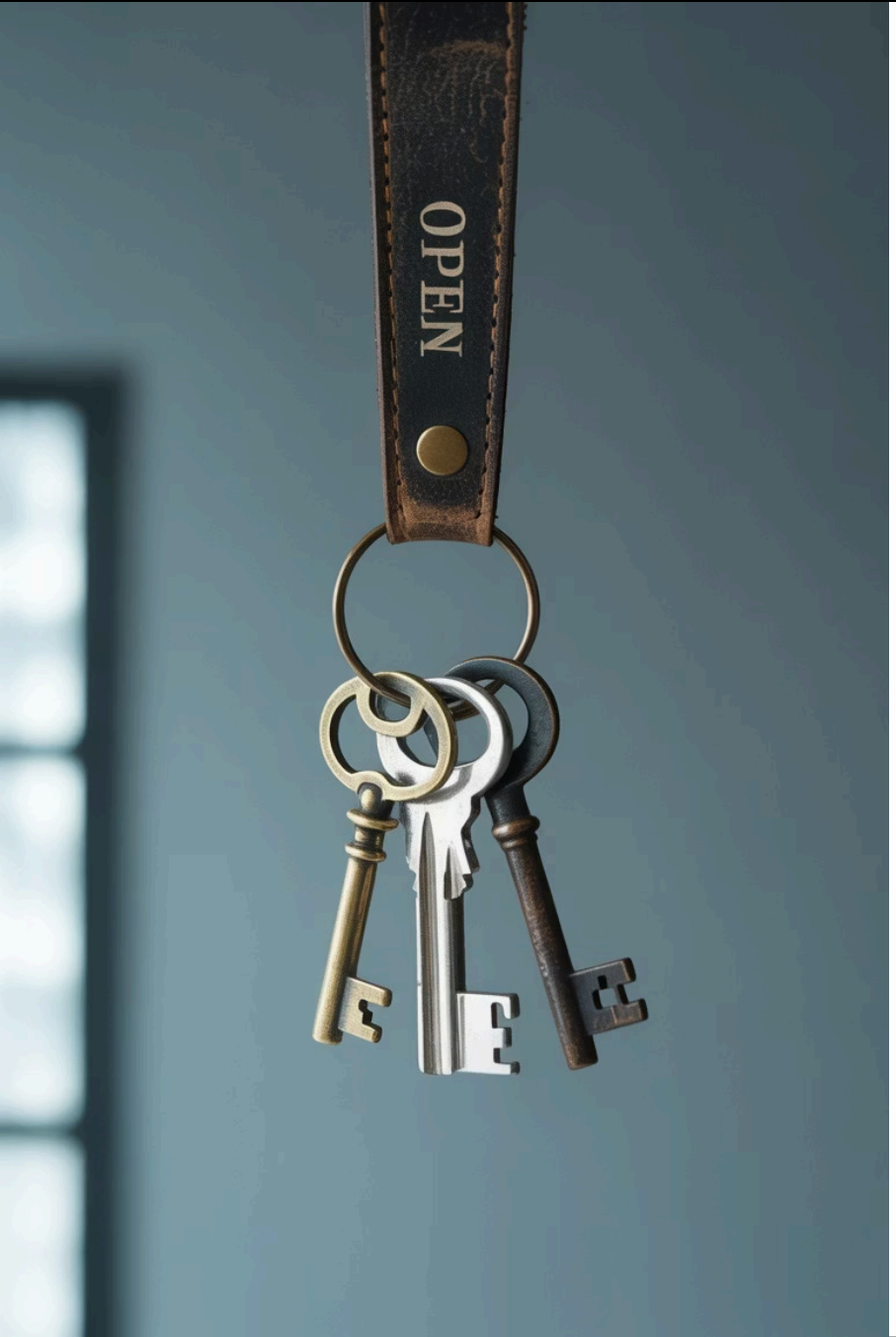
Your password is your first and most important line of defense. A weak password is like a cardboard door. The following principles will turn your passwords into a steel vault door.

# 📏 Length Trumps Complexity

Many believe that a short, complicated password like Xp8!z&a is super secure. This is a misconception. Computers can "guess" such short passwords extremely quickly (through so-called brute-forcing). A much better strategy is length.

**Imagine:** A short, but complicated knotted string is quickly cut. A very, very long, simple iron chain is much harder to overcome.

**The Rule:** A password should be **at least 12-15 characters** long. Longer is always better.




## 🎭 Uniqueness is Key

This is the **golden rule**: **Never use the same password for different services!**

Imagine having a single key for your front door, your car, your office, and your bank safe deposit box. If a thief steals that one key, they immediately gain access to your entire life. It's the same with passwords. If a website you used your "master key password" on gets hacked, attackers will immediately try that password on all other major services (Amazon, Google, PayPal, etc.).

**The Rule:** Every account gets its own, unique password.

# 🤔 The Recipe for a Strong Password

Creating a strong password is very easy if you have a method. The best method is the **Passphrase Method**.

01

## Think of a simple but long sentence

Only you know it, and it makes sense to you.

02

## Take the initial letters

Replace some words with numbers or symbols and deliberately include a "mistake".

**Example:**

- **Sentence:** "I walk my dog Fido every morning at 7 o'clock!"
- **Passphrase:** IgjMu7UmHFs!

This passphrase is long, unpredictable, and contains everything necessary.

# Weak vs. Strong Passwords

| Weak Password ❌ | Strong Password ✅ | Why it's Strong |
| --- | --- | --- |
| Anna1998 | My-Cat-likes-to-eat-mice!25 | Very long, easy to remember, mix of characters. |
| qwertz123 | 3_Cups:Coffee<per<Day | Long, unconventional, uses symbols as separators. |
| Sun2025 | Why1sTh1BananaCurv^d? | Long, uses substitutions (1 for i, Th for the), contains symbols. |

# 🔐 Password Manager: Your Digital Vault

Remembering dozens of strong, unique passwords is impossible. The solution is a **password manager**.

This is a program that functions like a digital, highly encrypted vault.

- [ ] ## One Master Password

  You only need to remember **a single, very strong master password**.

- [ ] ## Secure Storage

  The manager securely stores all your other passwords.

- [ ] ## Automatic Generation

  It can create extremely strong, random passwords for you and automatically insert them into websites.

Well-known and secure password managers include, for example, **Bitwarden** (free) or **1Password**.

# 🛡️ Protecting Personal Data and Handling Sensitive Information

Security goes beyond passwords. It's about how you behave in the digital space and to whom you entrust which information.

# 🤫 The Principle of Data Minimization

The safest data is the data you never give out in the first place. Always be suspicious if a website or app asks for more information than is necessary for its function.

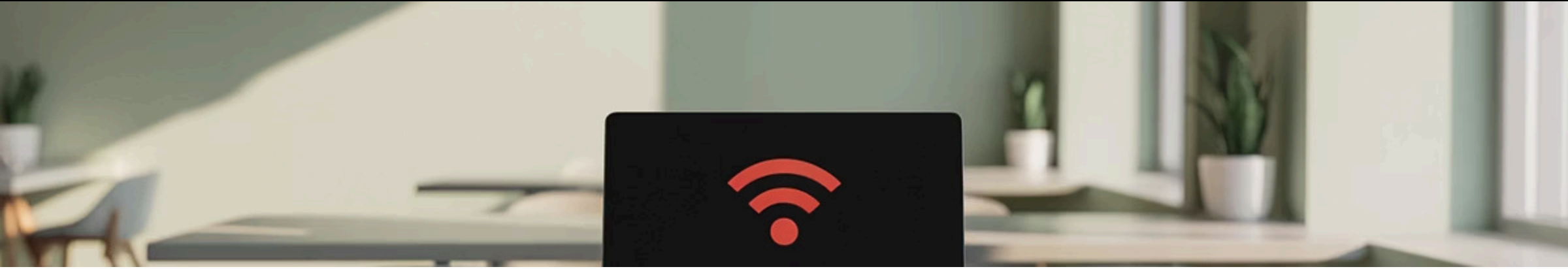
### Weather App

A weather app does not need your name or access to your contacts.

### Online Shop

An online shop does not need your date of birth to sell you a book.

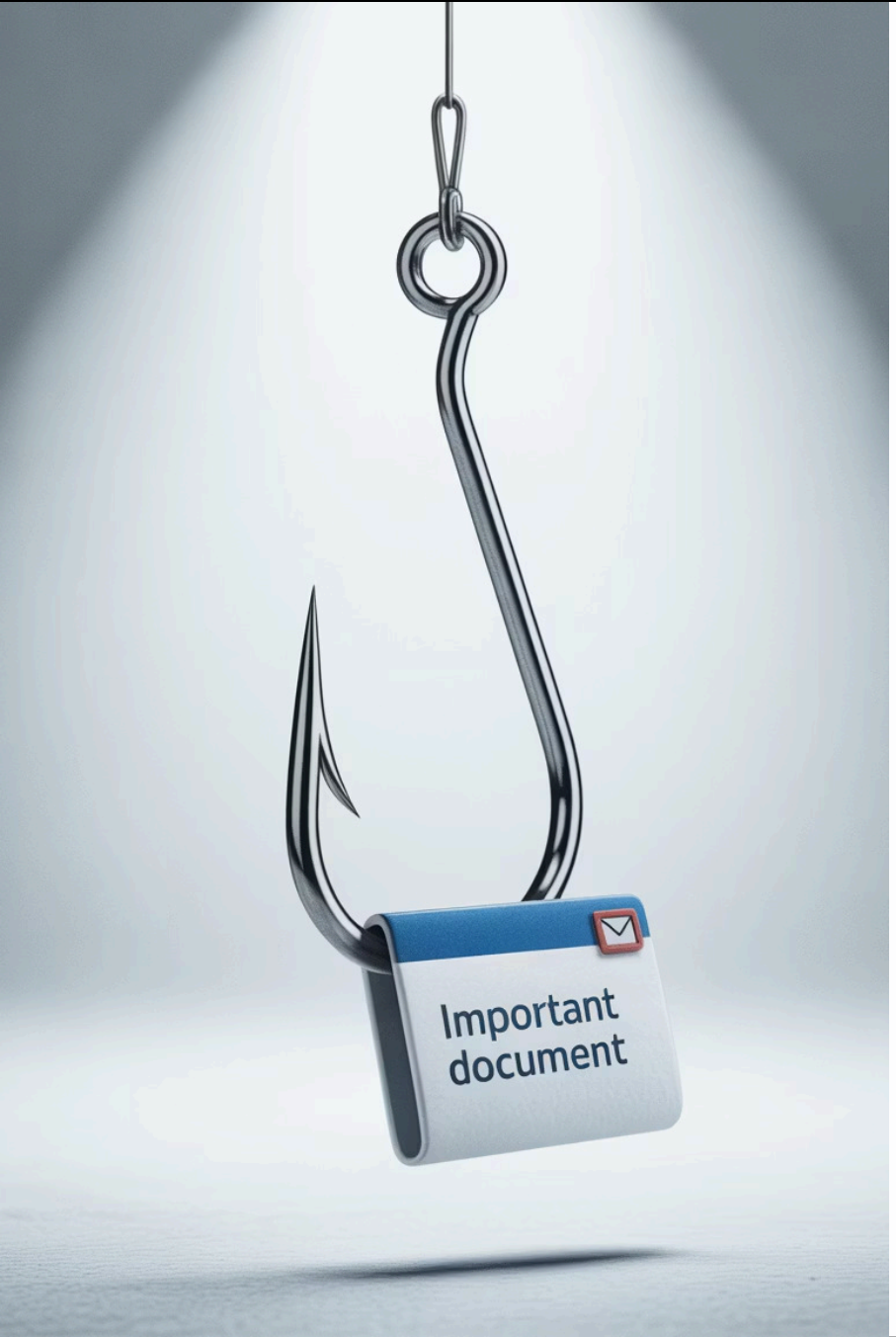
**The Rule:** Always disclose as little personal data as absolutely necessary. Always ask yourself: "Why do they really need this?"



# 🔍 Caution with Public Networks (Wi-Fi)

Public Wi-Fi in cafes, airports, or trains is convenient but potentially insecure. Since the connection is often unencrypted, it's easy for attackers on the same network to "eavesdrop" on your data—meaning they can read what you send and receive.

**The Rule:** Never perform sensitive activities like **online banking, shopping with a credit card**, or logging into important accounts on public Wi-Fi. Save these for a trusted network (e.g., at home). If it's unavoidable, use a **VPN (Virtual Private Network)**, which securely encrypts your connection.




# 🎣 Recognizing Phishing: Don't Be a Fish on the Hook

**Phishing** is an attempt by scammers to trick you into voluntarily revealing your sensitive data (like passwords or bank details). This usually happens via fake emails that look deceptively authentic.

# Typical Phishing Warning Signs

### Urgent Call to Action

You are asked to act **immediately** ("Your account will be blocked in 24 hours!", "Confirm your data now!").

### Threats or Unrealistic Promises

"If you don't click, a fee will be charged" or "You have won €1,000,000!".

### Impersonal Salutation

The email starts with "Dear Customer" instead of your name.

# Additional Phishing Warning Signs

### → Spelling and Grammar Errors

Reputable companies ensure correct language in their communications.

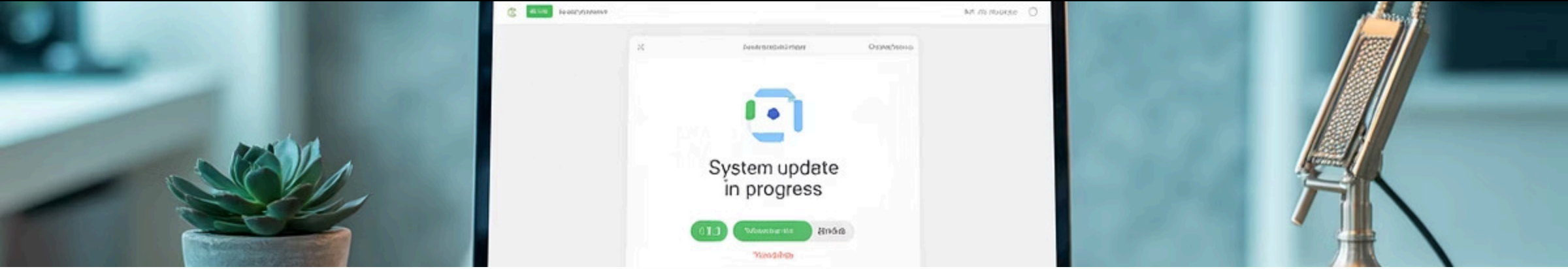
### → Strange Sender

The email address looks suspicious (e.g., paypal@service123.com instead of service@paypal.de).

### → Suspicious Links

The link in the text leads to a different address than displayed. Hover over the link with your mouse (without clicking!) to see the actual destination.

**The Golden Rule:** Never click on links or attachments in emails that you don't trust 100%. If in doubt, always go directly to the provider's website via your browser.




# 💻 Device and Software Hygiene

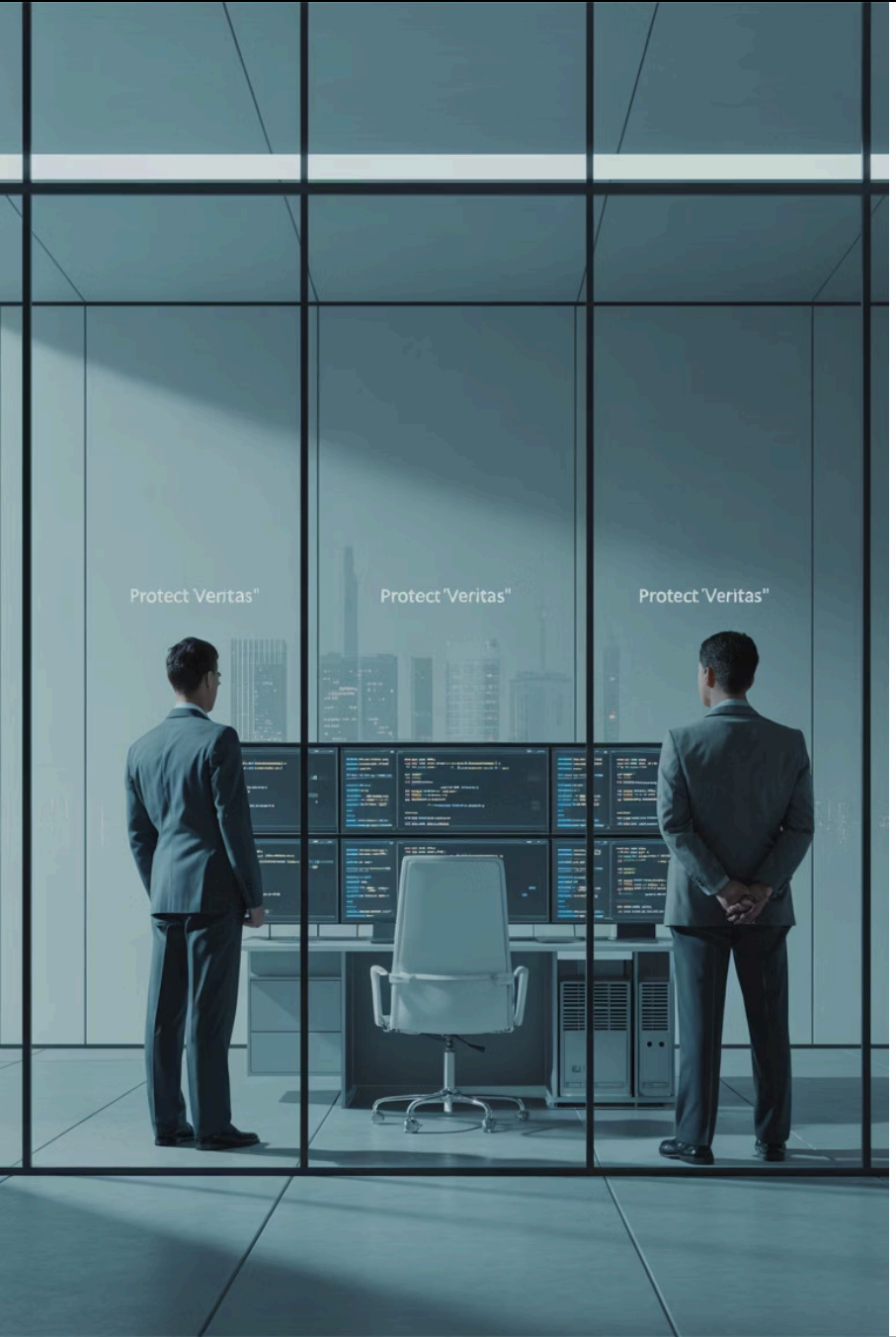
Your devices and programs are like your body – they need care to stay healthy and resilient.

## Updates, Updates, Updates

Keep your operating system (Windows, macOS), browser, and programs **always up to date**. Updates often close critical security vulnerabilities that attackers could otherwise exploit. Enable automatic updates wherever possible.

## Antivirus Protection

Good antivirus software is a must. It runs in the background and alerts you if a malicious file tries to sneak onto your computer. Modern operating systems like Windows 10/11 already have good basic protection integrated with "Defender."




# Antivirus & Maintenance

Imagine your computer as a house. Of course, you want to keep it clean, safe, and in top condition. Antivirus and maintenance are all the measures you take to prevent burglars (viruses), vandals (malware), and natural decay (security vulnerabilities). It's about proactively protecting your digital home instead of waiting until something breaks.

# 🛡️ Introduction to Antivirus Software and How It Works

## 👨‍⚕️ What is Antivirus Software?

Antivirus software is like a **security guard and a doctor** for your computer rolled into one.

### The Security Guard

It constantly monitors who or what is trying to access your computer – be it via email, download, or a USB stick.

### The Doctor

If your computer is already "infected" with a virus, the program can diagnose the illness (find the virus), quarantine it (isolate it), and, in the best case, remove it (cure it).

Modern operating systems like Windows 10 and 11 already come with "Microsoft Defender," a solid, tightly integrated antivirus solution.

# 🔬 How Does Antivirus Software Work?

Antivirus programs primarily use three methods to protect your computer. Think of them as three different investigation techniques:

## Signature-Based Detection (The Wanted List)

Every known virus has a unique digital "fingerprint," also known as a signature.

## Heuristic Analysis (Behavioral Analysis)

Analyzes program behavior and detects suspicious activities.

## Real-time Protection (The Guard at the Gate)

Monitors everything happening at the moment and intercepts threats immediately.

# 🔍 Signature-Based Detection in Detail

Your antivirus program has a huge database with the fingerprints of millions of known viruses – like a police wanted list.

1

## The Process

The program scans every new file on your computer and compares its fingerprint with the entries in the wanted list.

2

## Match

If there's a match, the program immediately raises an alarm.

3

## Updates

That's exactly why **daily updates** of your virus scanner are extremely important! This is the only way the wanted list is updated with the latest "mugshots."


# 🧠 Understanding Heuristic Analysis

What about brand new viruses that aren't yet in any wanted database? This is where heuristics come in.

**The Analogy:** Imagine a store detective. He doesn't know every thief personally, but he recognizes suspicious behavior – someone looking around nervously, putting on a jacket when it's warm, or quickly making something disappear into their pocket.

**The Process:** Similarly, antivirus software analyzes the **behavior** of programs. If an unknown piece of software attempts to perform suspicious actions (e.g., secretly modifying system files, sending itself to all email contacts, or encrypting the hard drive), heuristics become suspicious and block the program as a precautionary measure.

# 🛡️ Real-time Protection - The Guard at the Gate

This is the most important function in everyday use. Real-time protection is the active guard that stands at your computer's gate 24/7.

### The Process

It monitors everything that happens **in this moment**. It scans email attachments as soon as they arrive, checks files as you download them, and verifies programs the moment you start them.

### The Benefit

Threats are intercepted **before** they can even cause damage.

# ⚖️ Difference between Antivirus, Firewall, and Software Updates

Many people lump these three terms together, but they fulfill completely different, yet perfectly complementary, tasks. Imagine them as the three most important security features of your house:

| Component | 🏡 Analogy | 🎯 Main Task |
|---|---|---|
| 🛡️ **Antivirus** | The **security service INSIDE the house**. | **Finds, blocks, and removes** malicious software (viruses, Trojans, etc.) that tries to enter the house or is already inside. It inspects virtually every item and person in the house. |
| 🧱 **Firewall** | The **bouncer or the fortress wall** around the house. | **Controls the traffic** entering and leaving the house. It decides which "doors and windows" (network ports) may be open for communication with the outside world (Internet) and blocks all unwanted connection attempts from outside. |
| ⚙️ **Software Updates** | The **handyman repairing the windows and walls**. | **Closes security vulnerabilities**. Over time, experts discover small flaws ("holes" or "cracks in the wall") in software. An update is like the handyman bricking up these holes before an intruder finds them. |


# The Interplay of the Three Security Components

In summary:

### The Firewall

prevents uninvited guests from knocking on your door.

### The Antivirus Software

catches those who still manage to get to the door or whom you (accidentally) let in yourself.

### Software Updates

ensure that there are no secret shortcuts or broken windows through which someone could break in.

Only when all three components work together is your digital home truly well protected.

# 🛠️ Software Maintenance

Software maintenance encompasses all activities that ensure the programs on your computer are secure, stable, and up-to-date. This begins with the careful selection and installation of a program and extends to regular updates and clean removal when you no longer need it. Good software maintenance is a crucial building block for the health and security of your entire system.

# 📦 Safely Installing and Uninstalling Programs

Every new program on your computer is like a new roommate in your digital home. You should therefore know exactly who you're letting in and how to get rid of them without leaving any mess behind.

## 🛡️ The Safe Way to Install

Installing a new program is child's play, but precisely for this reason, mistakes often happen here that can later lead to problems.

# The Source is Crucial

The absolutely most important step is to download the program **only from a trustworthy source**.

### Optimal ✅

Always directly from the **official website of the manufacturer**. If you want to install "Firefox," go to www.mozilla.org.

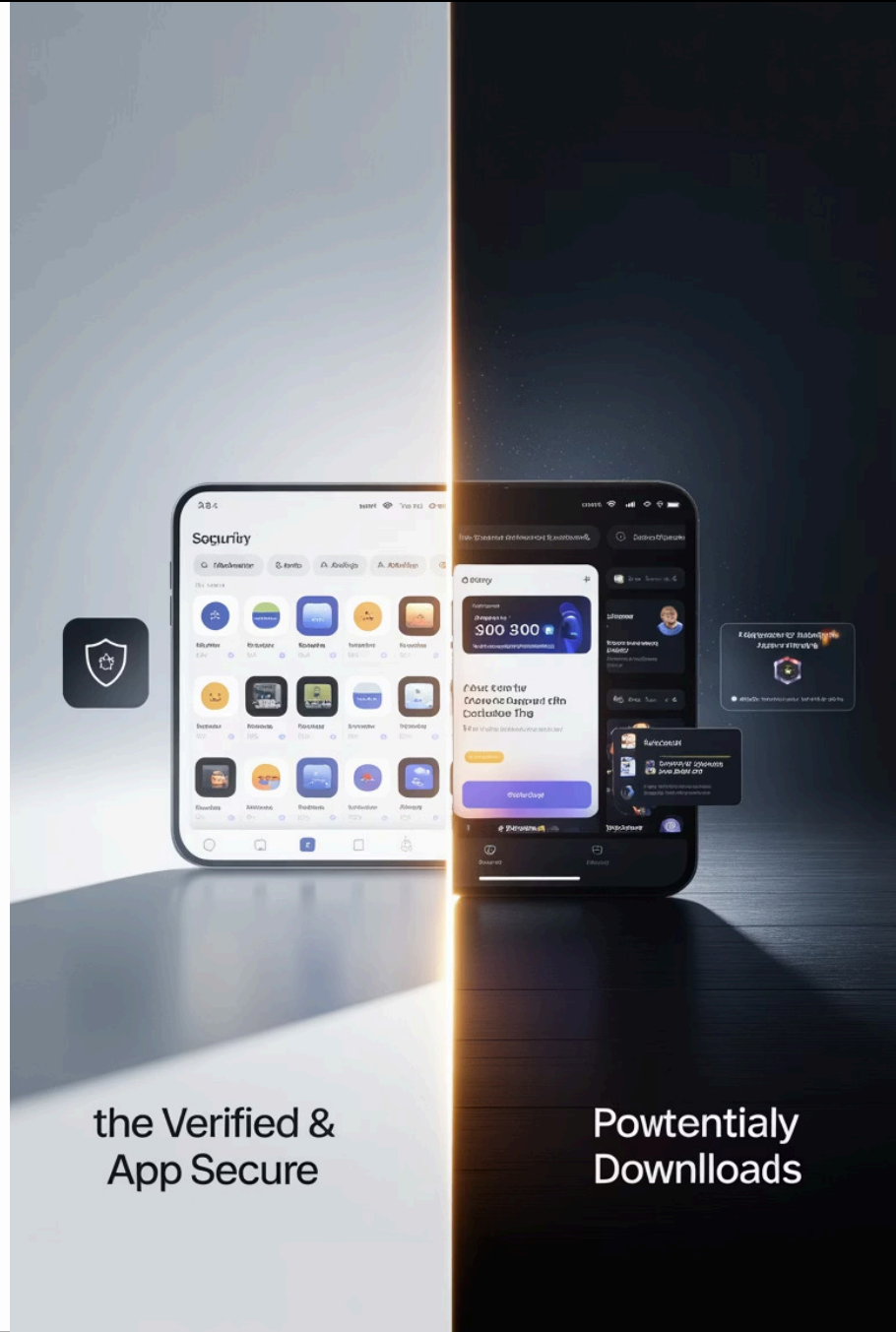
### Good ✅

Trustworthy app stores like the **Microsoft Store** or the **Mac App Store**.

### Dangerous ❌

Random download portals that advertise with "Free Download" buttons. These sites often finance themselves by trying to sneak unwanted additional software (adware, bloatware) onto your system.

**The Analogy:** You would rather buy a branded product from the manufacturer's official store than from a street vendor in a dark alley.



# Attention During Installation

Don't just blindly click through "Next, Next, Finish" during installation. Many untrustworthy programs hide small, pre-checked boxes in the installation process to install additional software you don't want (e.g., a different search engine for your browser or useless "PC optimization software").

1

## Choose Custom Installation

Select "Custom" or "Advanced" installation, if offered. This way, you can see exactly what is being installed.

2

## Read Each Step Carefully

Read each step carefully and uncheck anything you don't recognize or don't need.

# 🧼 Clean Uninstallation

If you no longer need a program, it is **not** enough to simply drag the program folder to the Recycle Bin! That would be like just driving the car out of the garage, but leaving all the junk, oil cans, and old tires behind.

A program leaves traces throughout the system: in the Windows registry, in configuration files, and in other system folders.

## Open System Settings

Go to your operating system's **System Settings**.

## Find the Apps Section

Look for the **"Apps"** or **"Programs and Features"** section.

## Select Program

You will see a list of all installed programs. Select the program you want to remove.

## Uninstall

Click the **"Uninstall"** button and follow the instructions.

This is the only way to cleanly and completely remove the program along with its digital "junk." This not only frees up storage space but also prevents potential conflicts with other software in the future.

# 🔄 Performing Software Updates and Understanding Their Importance

## 🤔 Why are Updates So Important?

Many people find updates annoying. "Not another update!". In reality, however, updates are a free and extremely important service provided by manufacturers. They have three main reasons:

| Reason | Analogy | Explanation |
|---|---|---|
| **1. 🔒 Close Security Gaps** | A **car recall**. | This is the **most important reason!** Sometimes experts discover flaws in a software's "blueprint" that hackers can exploit as secret entry points. An update is like a free trip to the workshop, where this dangerous vulnerability is repaired before an accident (a hacker attack) occurs. |
| **2. ✨ Get New Features** | A **free upgrade** for your product. | Developers have improved the program. You get new tools, a better user interface, or higher speed – completely free of charge. |
| **3. 🐞 Fix Errors (Bugfixes)** | The **repair of minor flaws**. | Sometimes a program crashes or a certain function doesn't work correctly. Updates fix these known errors ("bugs") and make the program more stable and reliable. |

A system without updates is like a medieval castle with an overgrown moat and leaky walls – an easy target for attackers.

# ⚙️ How do I perform updates?

Fortunately, updating is usually very easy these days.

## Automatic Updates (The best way)

Most modern programs and especially operating systems (Windows, macOS) are set to download and install updates **automatically in the background**. This is the safest and most convenient method. Check your settings to make sure this feature is enabled, and leave it on!

## Manual Updates (Proactive checking)

Some programs notify you with a small pop-up window that an update is available. For others, you have to be proactive. You can often find an option called **"Check for Updates"** or **"Update"** in the menu under **"Help"** or **"About"**. It's a good habit to do this once a month for programs you use frequently.

## App Store Updates

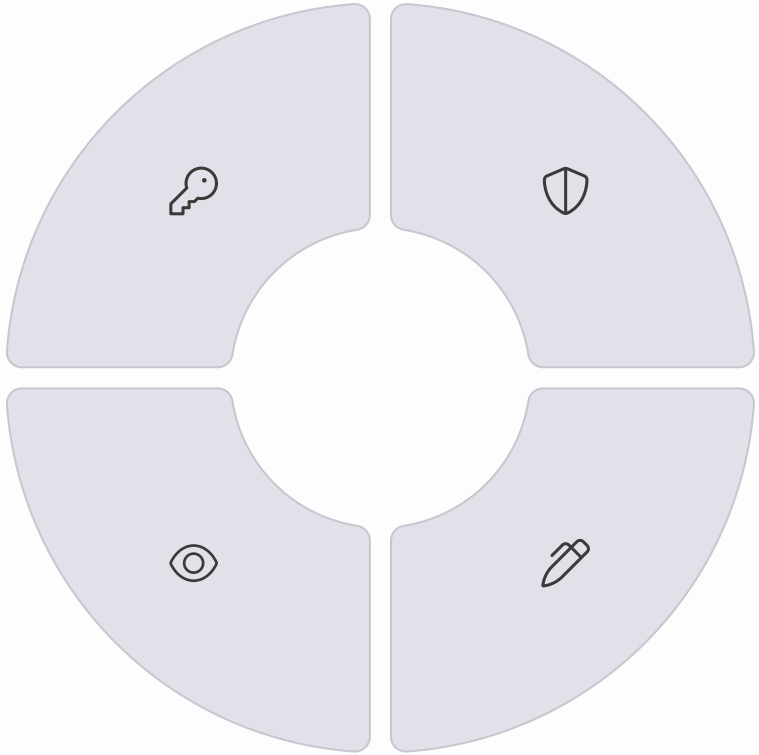
If you have installed programs from an App Store (e.g., Microsoft Store), the store centrally handles updates. There is usually a section called "Library" or "Updates" where you can see all pending updates and initiate them with a single click.

# 🔐 Summary: Your Digital Shield

IT security is not a one-time project, but a **daily habit**. Like brushing your teeth or locking the front door, these security measures should become routine.

### Strong Passwords

Long, unique, and managed with a password manager.



### Antivirus Protection

Active protection with up-to-date signatures and real-time monitoring.

### Vigilance

Recognize phishing and practice data frugality.

### Regular Updates

Automatic updates for operating system and programs.

With these fundamentals, you are prepared for most digital threats. Your digital treasure remains safely secured!