Securing Windows: The Practical Guide for Home Users

Excerpt – Chapter 1

Have you ever wondered why your Windows PC suddenly becomes a target for phishing attacks or ransomware, even with regular updates and antivirus software? In this hands-on guide, you'll learn step by step how to protect your machine with the same security measures used by large companies — no prior IT knowledge required.

Why Attacks Don't Just Hit Companies

Hardly a day goes by without reports of data breaches, ransomware gangs, or hacked online shops. The headlines often sound like they refer to corporations, government agencies, or hospitals — in other words, targets that already have IT professionals, budgets, and emergency plans. This gives many private individuals a fatal misconception: "This doesn't concern me. I have nothing to hide, and my computer is uninteresting to criminals anyway."

Both assumptions are wrong. Attackers don't think in categories like "important" or "unimportant." They think in numbers: anyone who can reach millions of private devices simultaneously with a single phishing wave doesn't have to pick each victim individually. It's enough if a fraction of them take the bait.

In addition, a typical Windows home computer today stores things that ten years ago were still in paper folders or photo albums. Tax returns, bank statements, scans of the ID card, health insurance numbers, login credentials for streaming services, family photos in the cloud. For criminals, this is an El Dorado — three examples from real life that happen in some form every day:

- **Ransomware on the family PC.** An extortion email pretends to come from a parcel delivery service. The attachment quietly encrypts the home computer. Suddenly, ten years of vacation photos and all Office documents are unreadable.
- **Identity theft after a data breach.** An online shop where you ordered something years ago suffered a data breach. The same email/password combination is also used for online banking — criminals test it on dozens of services.
- **Tech support scam on the phone.** A supposed Microsoft employee warns of a "critical infection" and asks for remote access via TeamViewer or Quick Assist.

All three cases have in common that no particularly deep technical knowledge was required to trigger them — a single careless click is enough. That is precisely why Windows security at home is not a specialist discipline, but a daily basic task, comparable to locking the front door.

> **Note.** Private users are not a peripheral topic of IT security, but a primary target. Automated attacks hit anyone who goes online. The difference lies not in "importance," but in preparation.

Phishing — Forged Messages with Real Damage

Phishing refers to the attempt to obtain confidential information through forged messages. The classic is an email asking for login data for your bank, PayPal, a parcel tracking service, or Microsoft 365. The links look legitimate at first glance, but lead to cloned websites. Today, the method works not only via email, but also via SMS ("smishing"), via WhatsApp messages, via QR codes on parking meters or notices, and increasingly via social media direct messages.

What makes phishing so dangerous is the mix of time pressure and personal address. Sentences like "Your account will be locked in 24 hours" are designed to prevent you from thinking calmly. Anyone who examines the message carefully will almost always find clues: a cryptic sender address, an unusual salutation, or a

domain like *bank-security-check.com* instead of the real bank's domain.

The complete book (14 chapters, PDF) is available for €9.99 at windows-absichern.de/en/ebook.html.