Sergey's Ultimate Hackproof Guide

SergeyPoltev

When it comes to cybercrime, there are always warning signs

Hackers and scammers never stop evolving their tactics but staying one step ahead is entirely possible. This guide equips you with the knowledge and tools to recognize, avoid, and defend yourself against today's most common digital threats.

How malware silently takes over your devices

Malware & Virus Threats: Malicious software that steals data, encrypts files, and hands criminals full control.

How to spot it:

- Device slows down, crashes, or overheats unexpectedly
- Random pop-ups, new toolbars, or browser redirects appear.
- Files go missing or you receive a ransom demand.

How to protect yourself:

- Install antivirus on every device — including your phone.
- Enable real-time protection, not just scheduled scans.
- Set antivirus definitions to auto-update — new threats emerge daily.
- Choose a solution with dedicated ransomware protection.

Check out my top picks for strong antiovirus: https://sergeypoltev.com/antivirus

How your personal data ends up in criminal hands

Data exposure: Hundreds of data brokers sell your address, phone, relatives, and financial profile — legally.

How to spot it:

- Scam calls or emails that use your full name.
- Your address or relatives appear on people-search sites.

How to protect yourself:

- Use an automated removal service; manual opt-outs don't last.
- Remove your data from broker sites, marketing lists, and court records.
- Run it ongoing. Brokers re-collect your data constantly.

Check out my top picks for data removal services (FREE SCAN) https://sergeypoltev.com/dataremoval

Did you know? This is a clickable PDF

Before you print, try clicking on any of the underlined words for more information on the topics listed.

Stay current on the latest threats.
https://sergeypoltev.com/

Most businesses don't know they've been breached until it's too late. Find out exactly where you're vulnerable in 5 minutes, free!
sergeypoltev.com/hackproof-score

How hackers spy on your internet traffic

VPN threats: Without encryption, your browsing, passwords, and data are visible on any network.

How to spot it:

- You use public Wi-Fi at airports, hotels, or cafes.
- Ads appear for things you searched but never bought you're being tracked.
- Your internet provider or employer can see every site you visit.

How to protect yourself:

- Use a VPN to encrypt all traffic on every device, every network.
- Always connect before using public Wi-Fi; unprotected hotspots are a hacker's playground.
- Choose a no-log VPN so your activity isn't stored or sold.

Check out my top picks for trusted VPNs: https://sergeypoltev.com/vpn

Why your inbox is an open book to Big Tech

Email privacy: Free email providers scan your messages, sell your data, and hand it over when asked.

How to spot it:

- You use Gmail, Outlook, or Yahoo for sensitive business communication.
- Ads appear based on topics you only discussed in email.
- Your email provider is based in a country with weak privacy laws.

How to protect yourself:

- Switch to an end-to-end encrypted provider like ProtonMail or Tuta even the provider can't read your messages.
- Choose a zero-knowledge service hosted outside data-sharing jurisdictions.
- Never send passwords, financial details, or client data over standard email.

Check out my top picks for private encrypted email: https://sergeypoltev.com/privateemail

How criminals steal your identity without you knowing

Identity theft: Fraudsters use your personal information to open accounts, take out loans, and drain your finances.

How to spot it:

- Bills or credit inquiries arrive for accounts you never opened.
- Your SIN or personal data appears on the dark web.
- Your credit score drops suddenly with no explanation.

How to protect yourself:

- Use an identity protection service that monitors your SIN and credit file 24/7.
- Place a credit freeze — it's free and stops anyone opening accounts in your name.
- Never carry your SIN card in your wallet.

Check out my top picks for Identity Protection: https://sergeypoltev.com/identityprotection

Sergey's Hackproof Tips

Did you know? Your phone is a hacker's favourite target. Most breaches start in your pocket. It knows everything about you and your business. The question is, who else does?

Discover the HackProof Phone.
https://sergeypoltev.com/hackproof-phone

How hackers turn your passwords against you

Credential theft: Stolen or reused passwords are the #1 cause of account takeovers.

How to spot it:

- Urgent login alerts for accounts you didn't access.
- A site looks real but the URL is slightly off.
- Emails or texts asking you to reset your password.

How to protect yourself:

- Use a password manager unique strong password for every account.
- Let it auto-fill — it only works on verified sites, blocking fakes.
- Enable MFA — a stolen password alone is never enough to get in.

Check out my top picks for Password Managers: https://sergeypoltev.com/passwordmanagers

Your phone knows everything about your business

Mobile privacy: Calls, messages, apps, and data on a standard phone are not built for business privacy.

How to spot it:

- Your standard phone shares location, app activity, and data by default.
- Sensitive business calls and messages pass through unprotected networks.
- Apps request access to your camera, mic, and contacts and you said yes.

How to protect yourself:

- Use a purpose-built secure phone with encrypted calls, messages, and apps.
- Take full control — decide exactly what can access your data and when.
- Keep sensitive business conversations off standard smartphones entirely.

Check out my top pick for Secure Mobile Phone: hhttps://sergeypoltev.com/phone-security

How criminals intercept your private conversations

Messaging threats: Standard SMS and chat apps trai

How to spot it:

- Sensitive business details sent over SMS, iMessage, or WhatsApp.
- No confirmation your messages are end-to-end encrypted.
- Your messaging app requires a phone number linking every message to your identity.

How to protect yourself:

- Use an app with end-to-end encryption only you and the recipient can read the message.
- Choose one that doesn't require a phone number no number means no link to your identity.
- Enable disappearing messages so sensitive conversations don't sit on a server indefinitely.

Check out my top pick for Secure Messaging apps: https://sergeypoltev.com/secure-messaging

Sergey's Hackproof Tips

Did you know? Digital pickpockets don't need to touch you.
Slip a Hack Proof Card™ in your wallet and they never get through.

Discover the HackProof Card.

https://sergeypoltev.com/hackproof-card