STAY SAFE ONLINE · 01 / 25

Stay Safe Online.

A practical starter guide for everyone. Ten minutes to read. Useful for the rest of your life.

FOR
Parents · kids · seniors · small businesses · anyone online

LENGTH
Thirteen numbered steps · about 10 minutes

Most people never had a lesson about online safety. Not in school. Not at work. Nowhere.

So when something bad happens online, they blame themselves. They should not. Nobody taught them what to look for.

This guide will not make you a security expert. It will give you the thirteen things that matter most, explained plainly. Read it once. Do what you can. Share it with someone who needs it.

You can be a grandparent, a parent, a teenager, or a small-business owner. This works for all of you.

Start here.

IF YOU ONLY DO THREE THINGS

01 **Set up passkeys on your important accounts**

02 **Install a password manager**

03 **Agree a family safe-word**

Do those and you are already ahead of most people. Then come back and read the rest.

Your accounts and passwords.

Most attacks start by stealing your password. These four steps fix that.

Use passkeys where you can.

01

A passkey is like a digital house key. It lives on your phone or computer. When you sign in, your device proves it is you. No password to remember. No password to steal.

Big services already support passkeys: Apple, Google, Microsoft, PayPal, Amazon, WhatsApp, GitHub, and many more.

DO THIS

The next time a site or app asks if you want to set up a passkey, say yes.

Turn on two-factor authentication, but skip SMS.

02

Two-factor authentication (2FA) means two steps to log in. Your password, plus one more thing. That “more thing” used to be a code sent by SMS.

SMS codes can be stolen. Criminals have learned how to trick phone companies into transferring your number to their own SIM. It is called SIM swapping, and it happens often.

DO THIS

Use an authenticator app. Good free choices: Microsoft Authenticator, Google Authenticator, Twilio Authy. Install one; follow the setup on your important accounts.

Any 2FA beats no 2FA. If SMS is the only option, still turn it on.

Use a real password manager.

03

If you reuse the same password in several places, one leak turns into many. Most people reuse passwords because remembering hundreds is impossible.

A password manager creates a unique, strong password for every site and remembers them for you. You only remember one main password.

DO THIS

Install one. Good choices: Bitwarden (free), 1Password, or KeePassXC. Browsers have built-in managers too, but dedicated apps are safer and work across all your devices.

Keep your devices updated.

04

Updates fix holes. Criminals scan the internet looking for devices that have not been updated. Those devices are the easiest targets.

DO THIS

Turn on automatic updates on your phone, your computer, and your apps. If your Wi-Fi router is older than five years, replace it — old routers stop receiving updates and become silent risks.

Spotting scams.

Scams in 2026 look good. Really good. AI helps criminals write messages that look legitimate in any language. The old advice (“look for bad grammar”) does not work any more.

Slow down before you click or scan.

05

Most scam messages try to make you panic. “Your package is waiting.” “Your account will be closed.” “Unusual activity detected.”

The trick is urgency. If you feel rushed, that is the moment to stop.

DO THIS

If a message tells you to click a link, don't. Open the app or the website yourself by typing the address. The same rule applies to QR codes on parking meters, restaurants, and flyers — criminals place fake QR codes over real ones.

Treat urgent messages from family or bosses with suspicion.

06

This is the scariest change in the last two years. Criminals can clone someone's voice from a short social media clip. They call you, sounding exactly like your son or your boss, asking for money in an emergency.

These calls are convincing. Even careful people fall for them.

> DO THIS
>
> Agree a safe word with your family. A normal word you wouldn't say in passing. If someone calls claiming to be a relative in trouble, ask for the safe word. If they can't say it, it's a scam. Hang up and call the real person back on their usual number.

For a boss or colleague, the same rule applies. Call back through a channel you already trust.

Learn the shape of investment scams.

07

The biggest financial fraud of the 2020s goes by several names: pig butchering, romance-investment scam, crypto scam. The pattern is always the same.

01	Someone messages you on social media or a dating app
02	They seem kind, interested, successful
03	Over weeks or months, they build trust
04	They mention a “great investment opportunity”
05	You invest a small amount, see fake profits
06	You invest more. Then more.
07	One day, the money is gone.

DO THIS

If anyone you met online — no matter how lovely they seem — ever mentions an investment platform, stop talking to them. No exceptions. Tell a friend or family member. These scams work because victims feel too ashamed to ask for help.

Protecting your data.

What leaks, what gets reused, and what you can share without later regret.

Check if your data has leaked.

08

Companies get hacked. Your email, your old passwords, and sometimes your address end up in databases that criminals share and trade.

There is a free service that tells you what has leaked about you.

DO THIS

Go to haveibeenpwned.com. Enter your email address. If anything has leaked, change those passwords and turn on passkey or authenticator 2FA for them.

Think before you share voice and photos.

09

Every short video with your voice, every photo of your face, every public vacation post is training material for someone else. Criminals use public clips to clone voices. Travel photos tell them when your home is empty. This is not a call to delete everything. It is a reminder to treat public posts as public.

DO THIS

Check your social-media privacy settings once a year. Set accounts to private if you want only friends to see them. Think twice before sharing voice notes in public groups. Turn off location tags on photos.

For families.

IV

Three conversations worth having before anyone in your house needs them.

Talk to teenage boys about sextortion.

10

This is painful to discuss. But silence is the bigger danger.

Teen boys are one of the most-targeted groups online in 2026. Someone pretends to be a girl their age, chats for a while, sends a picture, asks for one back, then threatens to share that picture unless the boy pays. Victims feel ashamed. Some have taken their own lives.

Modern versions use AI-generated images. The victim never actually sent a real photo. It does not matter to the criminal.

Tell them:

- If someone you meet online asks for a photo, stop talking to them
- If you are being threatened, do not pay. Paying does not stop it
- Do not delete the messages. They are evidence
- Tell a trusted adult immediately. We will not be angry

> **The “we will not be angry” part is the most important. Most teens stay silent because they are afraid of losing their phone.**

Teach children “stop, ask, tell.”

11

For children, online safety is not about technology. It is about a simple rule they can remember.

If anything online asks them for information, photos, or money — offers them gifts, games, or secrets — or feels strange, scary, or too good to be true:

1
Stop.
Do not reply. Do not click. Step away from the screen for a moment.

2
Ask.
A parent, a teacher, or another trusted adult. Show them the message.

3
Tell.
Tell someone if it keeps happening — the first person, or a different one.

DO THIS

Say the rule out loud with your child. Write it on a sticky note near the computer. Make sure they know you won't take the device away if they tell you. That fear is why most kids stay silent.

Verify unusual video calls.

12

In 2026, criminals can fake video in real time. A person on a video call might not be who they look like.

DO THIS

If anyone on a video call asks you to send money, share a password, or make an urgent decision that feels unusual, hang up. Call the person back on a number you already have saved. Verify through a second channel before you act.

One more thing.

When everything else fails, this is what lets you recover instead of rebuild.

Back up what you cannot lose.

13

Photos. Documents. Records. The things you would miss if your phone fell in a lake or your computer was stolen.

Follow the 3-2-1 rule.

3
Copies
Three copies of every important file. Two isn't enough — a copy that fails with the original isn't a copy.

2
Formats
Two different formats: cloud storage plus an external hard drive, for example. Diversify the risk.

1
Off-site
One copy in a different building, or in the cloud. If your house burns down, your photos survive.

DO THIS

Most phones and computers already handle the first two automatically if you enable iCloud, Google Drive, or OneDrive. Check yours is turned on.

Where to get help.

If something has already happened. Or is happening right now.

NEED HELP READING THIS?

Write to **education@webnestify.org** — we answer in Slovak or English.

In Slovakia

CYBERSECURITY	SK-CERT · sk-cert.sk · incidents, phishing, account compromise
FRAUD / THREATS	Your local police — for scams, extortion, anything criminal
FINANCIAL ATTACKS	Your bank's 24/7 fraud hotline · on the back of your card
KIDS & TEENS	Linka detskej dôvery · 116 111 · free, anonymous, 24/7

Across Europe

YOUR COUNTRY	Your national CERT or CSIRT
EU LEVEL	Europol · “Report Cybercrime” resource page
CONSUMER ISSUES	European Consumer Centre · cross-border scams

For suspected sextortion involving young people

REMOVE IMAGES	Take It Down · takeitdown.ncmec.org · removes stolen or AI-generated images before they spread

Thirteen steps. One page.

ACCOUNTS

01 · Use passkeys

02 · Authenticator 2FA, not SMS

03 · A real password manager

04 · Automatic updates; new router if yours is 5+ years old

SCAMS

05 · Slow down — type the address, don't click

06 · Safe-word for urgent family / boss calls

07 · “Investment tip” from online friend = walk away

DATA & FAMILIES

08 · Check haveibeenpwned.com

09 · Treat public posts as public; lock settings yearly

10 · Sextortion: don't pay, don't delete, tell an adult

11 · Kids: stop, ask, tell

12 · Unusual video calls — hang up and call back

RECOVERY

13 · 3-2-1 backups — three copies, two formats, one off-site

This guide is free. Pass it on.

Free to read, free to print, free to share. Send it to your family. Print it for your classroom. Translate it for your community. A short credit line (“source: Webnestify Education”) is appreciated but not required.

If we can help you deliver this as a workshop or a talk at your school, we will.

ONE

Print & share the guide

webnestify.org/stay-safe-online

TWO

Book a free workshop

education@webnestify.org

Webnestify Education, o. z.

A Slovak nonprofit making cybersecurity education accessible to everyone. We revise this guide whenever the threats change enough to matter.

VERSION
1.0

UPDATED
2026

LICENCE
Free

CONTACT
education@webnestify.org