

ZLEA DIGITAL SAFETY & CONSULTING

Free Digital Safety Guide

A short introduction to safer accounts, clearer privacy choices and healthier digital boundaries

FOR EVERYDAY INTERNET USERS

For individuals, families and young people who want to understand common digital risks without needing a technical background.

VERSION 1.0

This guide introduces the ZLEA free-resource library. Each topic links to a longer website article for readers who want practical steps.

START HERE

Digital safety begins with ordinary choices

Digital safety means protecting your accounts, devices, personal information and relationships when you use technology. It includes familiar actions, such as using a stronger sign-in method, and less obvious ones, such as checking who can still see your location after a relationship changes.

You do not need to fix everything at once. A few well-chosen changes can reduce the chance that one exposed password, one shared device or one forgotten setting gives someone lasting access to your digital life.

About the ZLEA website

ZLEA Digital Safety & Consulting is an accessible place for clear, practical guidance. The website brings together free resources, short news updates, a Get Help page and a newsletter for people who want to keep learning.

The aim is to make digital safety understandable to ordinary users, including parents, young people, women and girls, and anyone dealing with unwanted access after a friendship, family relationship or romantic relationship ends.

How to use this guide

- Read the short explanations on the next two pages.
- Choose one action that matters to you now.
- Use the Read the full article links when you want detailed instructions.
- Return to this guide when a device, account or relationship changes.

FREE RESOURCE LIBRARY

Three ways to strengthen your accounts

01 Multi-factor authentication

Let's suppose your password appears in a data breach. A second sign-in factor can stop the password from being enough on its own.

Multi-factor authentication, or MFA, asks for more than one kind of proof. A password may be followed by a code, a prompt, a passkey or a security key. MFA is especially important for email because email can reset many of your other accounts.

Start here: Turn on MFA for your main email account, then your financial and social accounts. Save the recovery codes somewhere other than your phone.

[Read the full article](#) on the ZLEA Digital Safety website

02 Authenticator apps

Let's suppose you change phone carriers and cannot receive text messages. An authenticator app can still generate your sign-in code.

Google Authenticator, Microsoft Authenticator and similar apps create short-lived codes on your device. They do not need a mobile signal to generate a code and are usually a stronger choice than text messages when a service supports them.

Start here: Lock your phone, plan how codes will move to a new phone, and keep account recovery codes in a safe separate place.

[Read the full article](#) on the ZLEA Digital Safety website

03 Google Account security

Let's suppose an old laptop is still signed in to your Gmail. Changing a password is useful, but reviewing signed-in devices matters too.

A Google security check should cover 2-Step Verification, recovery email, recovery phone, backup codes, recent security activity and connected devices. Each item supports a different part of access and recovery.

Start here: Visit myaccount.google.com from a trusted device. Remove unfamiliar devices and make sure every recovery method belongs to you.

[Read the full article](#) on the ZLEA Digital Safety website

FREE RESOURCE LIBRARY

Privacy, connections and digital boundaries

04 Google activity and data deletion

Let's suppose a private search from years ago is still saved in your account. You may want to review what is stored and for how long.

Google's history settings can include Web & App Activity, Timeline and YouTube History. You can delete selected items, delete a period of history, choose automatic deletion or pause some collection. Reduced history may also reduce personalization.

Start here: Review myactivity.google.com. If someone may still access the account, secure the account and its devices as well as deleting old activity.

[Read the full article](#) on the ZLEA Digital Safety website

05 VPN protection

Let's suppose you join unfamiliar public Wi-Fi. A VPN can protect the connection between your device and the VPN provider.

A virtual private network can hide your traffic from the local network and mask your device's public IP address. It does not stop phishing, remove malware or make you anonymous to a service where you sign in. The VPN provider becomes an important part of your trust decision.

Start here: Use a reputable provider, keep your software updated and continue using MFA and careful link-checking.

[Read the full article](#) on the ZLEA Digital Safety website

06 Digital breakup

Let's suppose a friendship, family relationship or romantic relationship has ended, but the other person still knows a passcode or has an old signed-in device.

Digital access does not expire when trust changes. Check email, recovery methods, active sessions, location sharing, phone and computer passcodes, shared albums, calendars, subscriptions and connected apps. This matters after any relationship change, not only a romantic breakup.

Start here: Secure email first. If the person may be abusive or monitoring a device, use a safer device, preserve evidence and seek support before making changes that could alert them.

[Read the full article](#) on the ZLEA Digital Safety website

FOR PARENTS AND CAREGIVERS

Help children build safety skills

Parental controls can help, but children also need language for uncomfortable situations and a trusted adult they can approach without fear of immediate punishment. Make online safety a regular conversation, not a single warning after something goes wrong.

A practical family approach

- Ask which apps, games and group chats your child uses. Explore settings together so supervision is clear rather than secret.
- Teach that passwords, one-time codes and recovery codes are private, even when a message appears urgent.
- Review location sharing, contact permissions, tagging and who can send direct messages. Use the child's real age so age-based protections can work.
- Before posting a child's photo, look for school names, uniforms, street signs, routines or live location clues. Ask older children before sharing their image.
- Explain impersonation, grooming, image-based abuse and threats in age-appropriate language. Make it clear that an offender is responsible for the abuse.
- If something happens, stay calm. Save relevant evidence, block and report when safe, and contact the platform, school or local support service as appropriate.

Questions worth asking

- If something online made you uncomfortable, would you feel safe telling me?
- Who can see your location, photos and private stories today?
- What would you do if someone asked for a secret photo, password or code?

If a child faces immediate danger, contact the appropriate emergency or child-protection service in your country. Laws and reporting options differ by location.

SELECTED UPDATES

Digital safety in 2026

Safety tools and online harms continue to change. These selected 2026 updates connect directly to the issues introduced in this guide. They are a starting point, not a complete news review.

10 FEB 2026 More family controls and built-in protections

Google and YouTube described easier Family Link controls, new limits for time spent scrolling YouTube Shorts, automatic wellbeing reminders for users under 18 and private-by-default uploads for creators aged 13 to 17. Tools can support a family plan, but they work best alongside regular conversations.

Source [Safer Internet Day USA - Google and YouTube family-safety update](#)

18 MAY 2026 Cyber violence follows girls across platforms

The European Institute for Gender Equality reported findings from focus groups with 133 girls and young women aged 13 to 18 in ten EU countries. Participants described exclusion and body shaming at younger ages, with sexualized and controlling abuse, deepfakes and grooming becoming more prominent among older girls.

Source [European Institute for Gender Equality](#)

JUN 2026 New consumer guidance on stalkerware

The US Federal Trade Commission published guidance on apps that can secretly track location, messages and device activity. It warns that removing monitoring software may alert an abusive person. Safety planning, a separate trusted device and preserving evidence may be important before changing the monitored phone.

Source [US Federal Trade Commission - Stalkerware What To Know](#)

Product features and menus can change. Check the official support page for the service you use before following a technical instruction.

YOUR NEXT STEP

Five actions for this week

- [] Protect your main email with a unique password and MFA.
- [] Confirm that recovery email addresses and phone numbers belong to you.
- [] Review signed-in devices and end sessions you no longer recognize or trust.
- [] Save backup codes somewhere separate from your phone.
- [] Review location sharing and other shared access after any relationship change.

Keep learning with ZLEA

The ZLEA Digital Safety website publishes practical articles, short updates and downloadable resources. Subscribe to the newsletter for clear reminders and new guides, or use the Get Help page when you need guidance on where to begin.

Contact zleadigitalsafety@gmail.com

Sources for the 2026 updates

[Safer Internet Day USA - Google and YouTube family-safety update, 10 February 2026](#)

[European Institute for Gender Equality - Growing up online, 18 May 2026](#)

[US Federal Trade Commission - Stalkerware: What To Know, June 2026](#)

This guide provides general educational information. It is not legal advice, emergency assistance or a substitute for support from a qualified local professional.