Safelygirlsecurity

WHAT WE CARRY TOOLKIT SERIES

Stay Savvy, Stay Safe

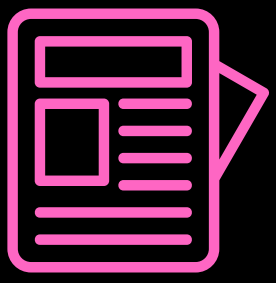
Your Ultimate Guide to Digital Defense

Table of Contents

Follow us!

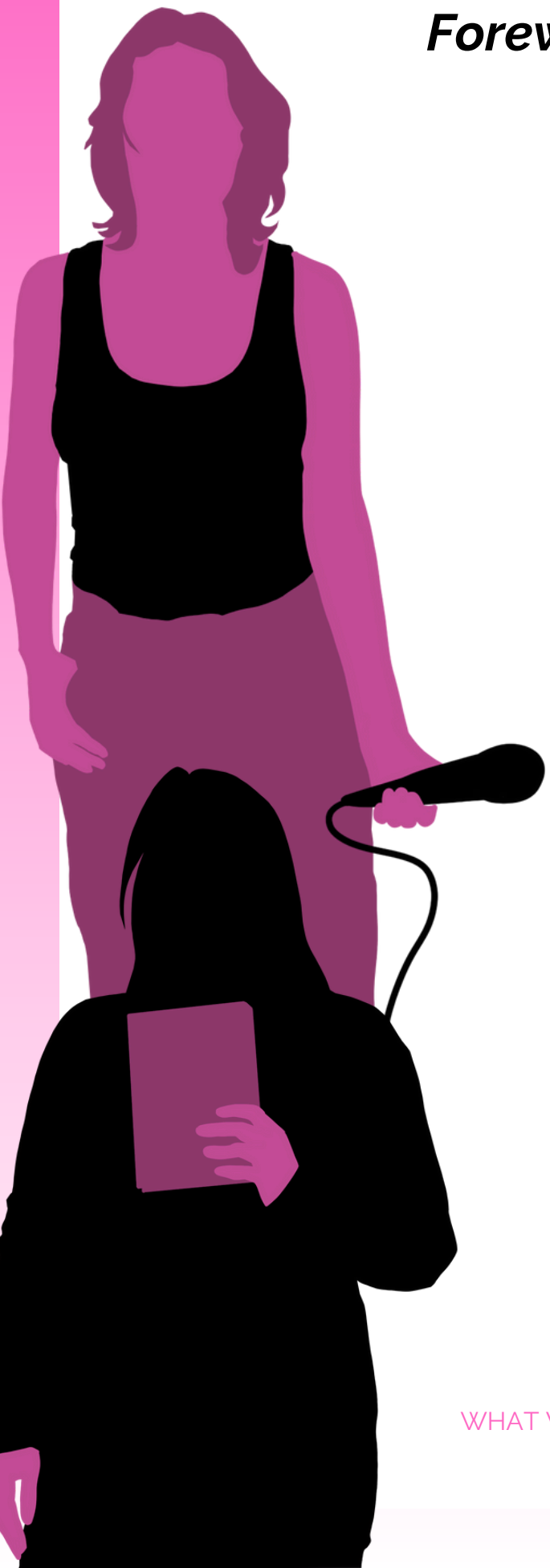
girlsecurity_

YouTube Link



Newsletter

girlsecurity.org



Foreword

At Girl Security, our approach to exploring national security considers multiple layers. Small "n" - national security - explores how girls and gender minority youth experience security challenges that originate in the homeland and national security domains but impact their understanding of personal security, such as physical violence and digital harms. Big "N" - National Security - explores the threats themselves and how they shape the United States and a global community. These challenges include war and conflict, threats arising from new technologies such as artificial intelligence, climate impacts, and biosecurity, for example.

In our work with girls and young women, and through surveys, participants identify a number of threats to their personal security (small "n" national security) including physical violence, cyberbullying, and school shootings. Participants often explain that they make themselves feel secure through several means, including their phones, some self-defense mechanism, and/or surrounding themselves with friends, family, and/or loved ones.

This guide is intended to provide frameworks for how girls consider their sense of personal safety and security and to strengthen their understanding of their inherent strengths and skills.

We want to thank our partners at **Safelyy** for their collaboration on this toolkit.

SECTION I:

Clickbait or Trap? Outsmart Phishing Scams

What is Phishing?

Phishing is like getting a fake message from a so-called "friend" who isn't who they say they are. Scammers create sneaky emails, texts, or DMs that seem super legit—like from your bank, favorite store, or even your school. They trick you into giving away personal info like passwords or credit card details. Spoiler alert: they're after your money or data.

Why Phishing is a Total Red Flag

- **Identity Theft:** They can steal your identity and use it for fraud.
- **Financial Loss:** They might empty your bank account or misuse your credit card.
- **Privacy Invasion:** They can access personal info, photos, and messages.

→ Examples

Romance Scams or Sweetheart Scams
Millions of people use online dating apps or social networking sites to meet someone. But instead of finding romance, many find a scammer trying to trick them into sending money.

Consider this scenario:

- 2 people start dating via a website or app
- Soon one person will want to email, call, or message the other off the platform
- They say it's true love, but they live far away — maybe for work or because they're in the military
- Then they start **asking for money.** Maybe it's for a plane ticket to visit the other person. Or emergency surgery that just popped up. Or something else urgent.

In 2022, nearly 70,000 people reported a romance scam, and reported losses hit a staggering **$1.3 billion.** The median reported loss: **$4,400.**

- Resource: The Federal Trade Commission (FTC)

→ Examples

Financial Scams

- While people often think older adults are more susceptible to scams, that isn't always the case.
- Generation Zers born between 1995 and 2012 are falling for online scams three times more often than Baby Boomers.
- Younger adults who grew up with technology use it and trust it more than tech-suspicious Boomers.
- **Gen Zers also have more of their finances online.** This makes it easy for con artists to access accounts and swindle money.
- The cost of falling for those scams may also be surging for younger people: Social Catfish's 2023 report on online scams found that online scam victims under 20 years old lost an estimated $8.2 million in 2017. In 2022, they lost $210 million.
  - Source: Vox
  - Behaviors such as **disclosing personal information (PII) like name, address, social security number, and/or sending money** create vulnerabilites.

How to Spot It

- **Sketchy Links:** Always hover over links before you click. If it looks off, don't click.
- **Too Good to Be True:** Did you really win a $1,000 gift card for doing nothing? Probably not. Be skeptical of anything that sounds too perfect.
- **Urgent Requests:** If an email demands immediate action or threatens consequences, it's a red flag.
- **Weird Addresses:** Legit companies won't email you from a weird address. Double-check who it's from. For example: https://www.girlsecurity.org/ is NOT girlssssecurity.net or girlsecurityisgreat.com

Protect Yourself

- **Don't Click:** If you're unsure, don't click the link. Go directly to the source (like your bank's website) to check.
- **Verify Requests:** If someone asks for sensitive info, verify by contacting the company directly.
- **Enable Two-Factor Authentication:** Add an extra layer of security to your accounts.

→ Remember: If something feels off, trust your gut! It's better to be safe than sorry.

SECTION II:

Bullying Behind Screens:
Shutting Down Cyberbullies

What is Cyberbullying?

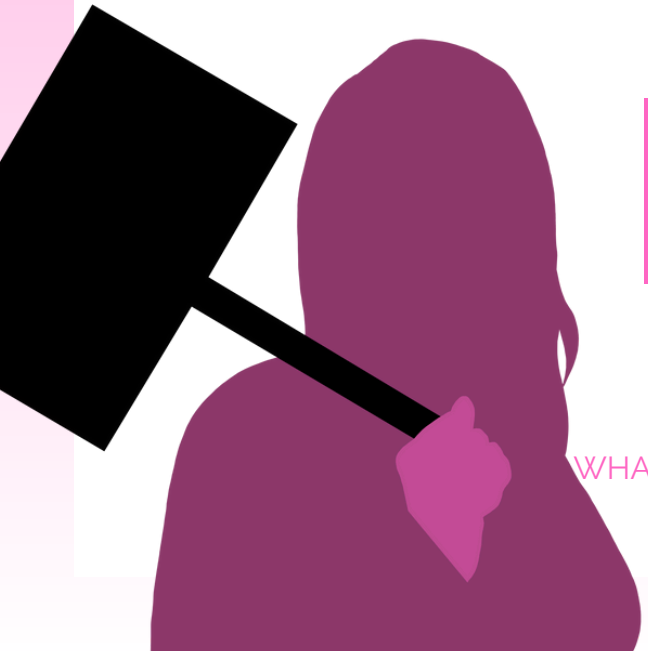
Cyberbullying is like regular bullying, but sneakier. It happens online through nasty comments, rumors, or threats sent via texts, social media, or even in gaming chats. It can mess with your mental health and self-esteem, making you feel isolated and alone.

Spotting Cyberbullying

- **Mean Messages:** Constant rude or threatening texts, DMs, or comments.
- **Public Shaming:** Someone posting embarrassing or hurtful things about you for others to see.
- **Impersonation:** Someone pretending to be you online to mess with your life.

How to Handle It

- **Screenshot & Save:** Keep evidence of the bullying, including messages, comments, and usernames.
- **Report & Block:** Report the bully to the platform and block them immediately. This prevents them from seeing your profile or posts, and makes it harder for them to get your information.
- **Talk It Out:** Reach out to someone you trust—like a friend, family member, or school counselor.
- **Don't Engage:** Engaging gives bullies power. Silence is golden.



Pro Tip: **Being online should be fun and safe.**
Don't let bullies ruin your vibe.
You have the right to stand up for yourself and others.

SECTION III:

Location on Lock: Why Sharing Your Whereabouts Isn't Worth It

What's Real-Time Location Sharing?

Real-time location sharing is when apps like Snapchat or Find My Friends show exactly where you are at any moment. It might seem cool to let your squad know where you're chilling, but it can also be risky. Always Posting your location in real-time is like sending out an open invite to anyone who sees your post.

The Risks

- **Strangers Watching**: If you're not careful, people you don't know (or don't trust) can track your every move.
- **Unwanted Attention:** Not everyone needs to know where you are 24/7—especially if it's someone who means you harm.
- **Privacy Invasion**: Even people you trust can overstep boundaries when they always know your location.

Staying Safe

- **Share Wisely:** Only share your location with people you trust completely, and limit how long they can see it.
- **Post After You've Left**: Share that amazing experience after you've left the place.
- **Be Vague About Location**: If you have to post, don't tag the exact spot.
- **Use Ghost Mode**: On apps like Snapchat, use Ghost Mode to keep your location private.
- **Check Your Settings**: Regularly review your app settings to see who has access to your location.

Why It's Worth It

Keeping your location private is about controlling your space and safety. It's cool to be connected, but it's also cool to stay safe and in control of your personal info.

Conclusion: Stay Smart, Stay Secure

Remember, being online is awesome and navigating the digital world doesn't have to be a minefield. By staying aware of the dangers like **phishing, cyberbullying,** and **oversharing your location,** you can protect yourself and your peace of mind.

Remember, it's your digital life—own it, protect it, and don't let anyone take that power away from you. If you ever feel unsure, trust your instincts and take steps to verify.