Everyday tips to to Keep You *Safe Online*

Online safety isn't just for experts. It's about small habits that keep your digital life secure every day. **Cybersecurity isn't about one magic solution;** it's about layering protections to cover all your bases.

Think of it like locking every door and window in your house; leaving just one open gives attackers an entry point

12 THINGS YOU SHOULD NEVER DO ONLINE

1. **Reuse passwords across accounts:** If one account gets hacked, all your accounts are at risk.
2. **Connect to public WiFi without a VPN:** Hackers can intercept your data on unsecured networks.
3. **Skip software updates:** Outdated software leaves you vulnerable to known exploits.
4. **Click links in random DMs or emails:** These are often phishing attempts to steal your info.
5. **Post real-time location on stories:** It reveals your exact whereabouts to strangers.
6. **Leave Bluetooth on in public spaces:** Hackers can exploit open connections to access your device.

COPYRIGHT © CYBERSECURITY GIRL - ALL RIGHTS RESERVED.

7. **Give every app camera/mic access:** Apps can misuse these permissions to spy on you.
8. **Use the same email for every login:** A breached email compromises all linked accounts.
9. **Skip two-factor authentication (2FA) because it's "annoying":** It's a critical extra layer of protection against hackers.
10. **Ignore privacy settings on social media:** Leaving them open exposes your personal info to anyone.
11. **Use "free" apps without reading what data they collect:** Many "free" apps profit by selling your data.
12. **Forget to delete old online accounts:** Unused accounts are easy targets for hackers.

WHY IT MATTERS

Avoiding these twelve online mistakes is crucial because together **they close off the most common ways hackers and scammers exploit vulnerabilities**. By combining these habits, you're building a strong, holistic defense that makes you a much harder target for cybercriminals. It's about creating a culture of security in your daily life.

COPYRIGHT © CYBERSECURITY GIRL - ALL RIGHTS RESERVED.

WHAT TO DO AFTER A DATA BREACH?

When your data's leaked in a breach, here's exactly what I recommend you do next:

1. **Change your password** for the account (and anywhere else it was reused)
2. **Turn on two factor authentication** for that account
3. **Freeze your credit** so no one can open accounts in your name

HOW DO YOU FREEZE YOUR CREDIT?

Freezing your credit is an essential step to protect yourself from identity theft, and it's super easy to do!

You'll need to contact all three major credit bureaus, Equifax, Experian, and TransUnion, individually to request a freeze (you can also temporarily lift the freeze if you need to apply for credit).

SEE THE TABLE ON THE NEXT PAGE

COPYRIGHT © CYBERSECURITY GIRL - ALL RIGHTS RESERVED.

HOW DO YOU FREEZE YOUR CREDIT?

BUREAU	PHONE	ONLINE
EXPERIAN	1-888-397-3742	equifax.com/freeze/center.html
EQUIFAX	1-888-298-0045	equifax.com/personal/credit-report-services/credit-freeze/
TRANSUNION	1-888-909-8872	transunion.com/credit-freeze

WHY IT MATTERS

Freezing your credit is like putting a lock on your financial identity, preventing scammers from opening credit cards, loans, or accounts in your name without your permission. Even if your personal information is leaked in a data breach, a credit freeze ensures that criminals can't use it to wreak havoc on your finances. **It's a simple but powerful way to protect yourself from identity theft!**

COPYRIGHT © CYBERSECURITY GIRL - ALL RIGHTS RESERVED.