DIGITAL SECURITY GUIDE

Protect Your Privacy, Data, and Identity Online

Created by Live Laugh Love Do

www.livelaughlovedo.com

Welcome to Digital Security!

In 2024, cybercrime cost victims over $12.5 billion. Data breaches exposed billions of records. Identity theft ruined credit scores and bank accounts. Scammers tricked people out of life savings.

You are a target. Whether you realize it or not, hackers, scammers, and data brokers are after your information right now.

The good news? Most cyber attacks succeed because of simple mistakes—mistakes this guide will help you avoid. You don't need to be a tech expert. You just need to follow basic security principles.

The 4 Pillars of Digital Security:

1. **STRONG AUTHENTICATION:** Unbreakable passwords and two-factor authentication
2. **PRIVACY CONTROL:** Limit what data companies and people can access
3. **THREAT AWARENESS:** Recognize scams, phishing, and social engineering
4. **SECURE DEVICES:** Protect phones, computers, and networks from attacks

50-Point Digital Security Checklist

Complete these tasks to dramatically improve your security (2 hours total)

PASSWORD SECURITY (10 items)

■ Use a password manager (1Password, Bitwarden, Dashlane)

■ Change all passwords to unique, 16+ character combinations

■ Enable two-factor authentication (2FA) on all major accounts

■ Use authenticator app (not SMS) for 2FA when possible

■ Never reuse passwords across different sites

■ Check if your emails/passwords were in data breaches (HaveIBeenPwned.com)

■ Set up security questions with false answers (store in password manager)

■ Remove saved passwords from browsers (use password manager instead)

■ Create secure master password you'll never forget

■ Share password manager vault with trusted family member (emergency)

DEVICE SECURITY (10 items)

■ Enable full-disk encryption on all devices

■ Set up biometric authentication (fingerprint/face ID) plus strong PIN

■ Install reputable antivirus software

■ Enable automatic software updates

■ Cover webcam with physical cover or tape

■ Disable Bluetooth/WiFi when not in use

■ Set devices to auto-lock after 1-2 minutes

■ Enable "Find My Device" on all phones/tablets/laptops

■ Back up important data to encrypted external drive

■ Wipe old devices before selling/donating (factory reset twice)

ONLINE PRIVACY (10 items)

■ Review and tighten privacy settings on all social media

■ Limit who can see your posts, friends list, and personal info

■ Remove personal info from data broker sites (Spokeo, WhitePages, etc.)

■ Use privacy-focused browser (Firefox, Brave) or privacy extensions

■ Install ad blocker and tracker blocker extensions

■ Disable location tracking on apps that don't need it

■ Review app permissions on phone (camera, microphone, contacts)

■ Opt out of data sharing in device settings

■ Use VPN when on public WiFi or for privacy

■ Use separate email for online shopping/spam (not personal email)

How to Spot Scams & Phishing

Red flags that indicate fraud—never ignore these warning signs:

Scam Type	Warning Signs	What to Do
Phishing Email	Urgent language, generic greeting, suspicious sender, requests for passwords/payment, threats	Delete immediately. Never click links. Verify by contacting company direc
Phone Scam	Unsolicited call about IRS/tech support/prizes, pressure tactics, asks for payment or personal info	Hang up. Real agencies never call asking for immediate payment. Call of
Romance Scam	Quick declarations of love, avoids meeting in person, asks for money (emergency, travel), too good to be true	Stop contact. Never send money. Report to dating site and FBI IC3.
Tech Support Scam	Pop-up warning of virus, unsolicited call about computer problems, requests remote access	Close browser. Legitimate companies never cold-call. Run your own anti

Emergency Response: If You've Been Hacked

Act immediately if you suspect your accounts or identity have been compromised:

IMMEDIATE ACTIONS (First 24 Hours):

1. **Change all passwords** starting with email, banking, and critical accounts
2. **Enable 2FA** everywhere if not already active
3. **Check bank/credit card statements** for unauthorized transactions
4. **Run full antivirus/malware scan** on all devices
5. **Alert your bank** if financial accounts affected
6. **Place fraud alert** on credit reports (call one bureau, they alert others)
7. **Document everything** - screenshots, emails, transaction records

NEXT STEPS (Week 1):

8. **File police report** for identity theft
9. **Report to FTC** at IdentityTheft.gov
10. **Freeze credit** at all three bureaus (Equifax, Experian, TransUnion)
11. **Check all accounts** for suspicious activity or new accounts
12. **Update security questions** to false answers only you know
13. **Review email forwarding rules** and authorized apps
14. **Consider identity theft protection service**

Stay Vigilant, Stay Secure

Digital security isn't a one-time task—it's an ongoing practice. Threats evolve, new scams emerge, and technology changes. But the fundamentals remain the same:

Use strong, unique passwords.
Enable two-factor authentication.
Think before you click.
Keep software updated.
Trust your instincts.

If something feels off, it probably is. Take the time to verify. Better to be paranoid than compromised.

Your digital life is worth protecting. Stay safe out there! ■