Staying Safe in a Digital World

"A prudent man foresees evil and hides himself, But the simple pass on and are punished." Proverbs 22:3

Scammers now use AI to write perfect emails, build fake websites, and copy the voices of people we love. Americans reported nearly **$900 million** lost to AI-related scams last year. Meanwhile, faulty software updates have recently knocked out email, airlines, and flight control for hours. A few simple habits go a long way.

Part 1: Protect Your Digital Life

1. **Pick a family code word.** Choose a secret word only your family knows. If a "grandchild" calls crying for money, ask for the word. AI can copy a voice from just a few seconds of video posted online.
2. **Hang up and call back.** If someone claims to be your bank, the IRS, police, tech support, or a relative in trouble, hang up. Call back using a number you already have, like the one on your card or in your contacts.
3. **Know the red flags.** Pressure to act *right now*, a request to keep it secret, or payment by **gift cards, wire transfer, cryptocurrency, Bitcoin ATM, or a cash courier**. No real business or government agency asks for these.
4. **Don't click links in surprise texts or emails.** "Your package is delayed" or "Your account is locked" messages are often fake. Open the app or type the website yourself.
5. **Use a different password for every account.** Most break-ins happen because a password leaked from one site and was reused on another. Use long passphrases (three or four random words), and consider a password manager. Change any password you have reused.
6. **Turn on two-step login,** especially for email and banking. Even if a thief has your password, they cannot get in without the code from your phone. Never read that code to anyone who calls you.
7. **Freeze your credit** with all three bureaus (Equifax, Experian, TransUnion). It is free, stops thieves from opening accounts in your name, and you can lift it any time.
8. **Keep updates on, but back up first.** Updates fix security holes. Back up photos and files regularly so a bad update can't take them. When a big service goes down, it is usually an outage, not an attack. Be patient and wait for news from the company itself.
9. **Post less of your family online.** Short videos and voice clips can be used to clone voices. Set social media accounts to private.
10. **Turn on bank alerts.** Get a text or email for every charge so you notice fraud fast.

Part 2: Be Ready at Home

When card readers, ATMs, phones, or the internet go down, whether from an outage, a bad update, an attack, or a storm, these steps keep your household going.

- ☐ **About a week of cash** in small bills ($1s, $5s, $10s, $20s), kept somewhere safe at home
- ☐ **A paper list** of important phone numbers: family, doctors, pharmacy, bank, insurance, and church
- ☐ **A paper list of medications** and doses; refill prescriptions before you run low
- ☐ **Gas tank at least half full.** Pumps need power and working card readers.
- ☐ **Water and food** for several days (about 1 gallon of water per person per day)
- ☐ **Flashlights, a battery or hand-crank radio,** spare batteries, and a charged power bank for phones
- ☐ **Paper copies of key documents** (IDs, insurance cards, recent bank statements) in a folder you can grab
- ☐ **Check on neighbors and church family,** especially those who live alone

If You Think You've Been Scammed

1. **Stop.** Don't send more money, even if they threaten you.
2. **Call your bank or card company** using the number on your card. Ask them to stop or reverse payments.
3. **Change your passwords,** starting with email and banking.
4. **Report it.** Reporting helps investigators and may help you recover money.
5. **Don't be embarrassed.** These scams fool smart, careful people every day.

Helpful Resources (Anywhere in the U.S.)

Need	Where to go
Report online fraud or scams	FBI: **ic3.gov**
Report fraud, get a recovery plan	FTC: **reportfraud.ftc.gov** and **identitytheft.gov**
Help for seniors and caregivers	National Elder Fraud Hotline: **1-833-372-8311**
Free credit freeze	**equifax.com**, **experian.com**, **transunion.com**
Free credit reports	**annualcreditreport.com**
Check if your email was in a breach	**haveibeenpwned.com**
Stop unwanted sales calls	**donotcall.gov** or **1-888-382-1222**
Emergency preparedness lists	**ready.gov**

Questions or need help with any of this? Talk to one of our deacons. We're glad to sit down with you and walk through it.

"Watch, stand fast in the faith, be brave, be strong." 1 Corinthians 16:13