CYBERSAFE SENIORS – EMERGENCY ACTION GUIDE

1. If You Clicked a Suspicious Link

Follow these steps immediately:

1. **Do NOT enter any personal information.**
2. **Disconnect from the internet** (Wi-Fi and mobile data).
3. Open your antivirus program and **run a full scan**.
4. **Change your passwords** for email, banking, and important accounts.
5. **Watch for unusual activity** on your accounts for the next 7 days.

---

2. If You Entered Personal or Financial Information

Take urgent action to protect your identity:

1. **Change your password immediately.**
2. Turn on **Two-Step Verification** (MFA).
3. If you entered bank/credit card info, **call your bank's fraud department**.
4. Check your **credit report** for new accounts you didn't open.
5. Report identity theft to the FTC:
   ➤ **IdentityTheft.gov**

---

3. If You Think Your Bank Account Is Compromised

Act quickly to protect your money:

1. **Call your bank's fraud hotline right away.**
2. Ask the bank to **freeze your card or account** if needed.
3. Review recent transactions and **report anything suspicious.**
4. Consider placing a **Fraud Alert** on your credit report.
5. Report fraud to the FTC:
   ➤ **ReportFraud.ftc.gov**

---

4. If Your Device Is Acting Strange

Signs: pop-ups, slow performance, unknown apps, unusual messages.

1. **Disconnect from the internet.**
2. Run a **full antivirus scan**.
3. Delete apps or programs you don't recognize.
4. **Don't enter passwords** until your device is secure.
5. Contact a **trusted IT technician** if problems continue.

---

5. Important Emergency Contacts

Bank Fraud Hotlines

- **Chase:** 1-800-935-9935
- **Bank of America:** 1-800-432-1000
- **Wells Fargo:** 1-800-869-3557
- **Citibank:** 1-800-950-5114

Credit Bureaus

- **Equifax:** 1-888-766-0008
- **Experian:** 1-888-397-3742
- **TransUnion:** 1-800-680-7289

Government & Reporting

- **FTC Fraud Hotline:** 1-877-382-4357
- **Identity Theft Reporting:** IdentityTheft.gov
- **FBI Cybercrime Reporting:** ic3.gov

---

6. Quick Safety Tips

- **Never click links** from unknown texts or emails.
- **Use strong passwords** and enable 2-step verification.
- Keep your **devices updated**.

- Install **trusted antivirus software**.
- If unsure, **ask a trusted family member or tech helper**.

---

7. Keep This Guide Handy

Print this page and place it near your:
✓ Computer
✓ Phone
✓ Router
✓ Workspace

It will help you act quickly in case of a cyber emergency.