Emergency Cyber Safety Guide for Seniors

1. If You Clicked a Suspicious Link

- Close the website or pop-up immediately.
- Do NOT enter any information.
- Disconnect Wi-Fi or mobile data temporarily.
- Run a quick device security scan.
- Change passwords for important accounts.
- Turn on Two-Factor Authentication (2FA).
- Watch for strange login alerts or emails.

2. If You Entered Sensitive Personal Information

- Change your password immediately.
- Enable 2FA on all major accounts.
- If you entered credit card info, call your bank and freeze the card.
- If you entered your Social Security number, freeze your credit.
- Report the scam to the FTC: https://reportfraud.ftc.gov/
- Monitor accounts for unusual activity.

3. If You Think Your Bank Account Is Compromised

- Call your bank immediately (use the number on your card).
- Request a temporary freeze on your account.
- Change your online banking password.
- Review recent transactions for fraud.
- Turn on alerts for withdrawals and logins.
- Report major losses to the FBI IC3: https://www.ic3.gov/

4. If Your Device Is Acting Strange

- Restart your device.
- Install the latest software updates.
- Run antivirus or security scans.
- Delete apps or browser extensions you do not recognize.
- Change important passwords.
- Ask a trusted family member or technician for help if problems continue.

5. Important Contact Numbers

- Bank of America: 1-800-432-1000
- Chase: 1-800-935-9935
- PNC Bank: 1-888-762-2265

- Equifax Freeze Line: 1-800-349-9960
- Experian Freeze Line: 1-888-397-3742
- TransUnion Freeze Line: 1-888-909-8872

- FTC Fraud Reporting: https://reportfraud.ftc.gov/
- FBI Internet Crime Center (IC3): https://www.ic3.gov/