Diversified

EXPERIENCE LIFELONG WEALTH

What To Do If Your Security Has Been Compromised

- ☐ **Contact your financial institutions immediately**. Alert your banks, creditors, and cell phone company that your security has been compromised, and follow any steps recommended to secure your account. This may include requesting new debit and credit cards and placing temporary holds on accounts to prevent new services (such as phone lines and devices) from being opened in your name.

- ☐ Contact one of the three main credit bureaus to **place an initial fraud alert on your credit report**. This will not prevent you from opening new accounts, but will require creditors and service provider to take additional steps to verify your identity before opening new accounts, requesting additional cards, or increasing credit limits. If you want extra protection, you can **contact each bureau individually to request a credit freeze**. This will disable any creditor from accessing your credit until you lift the freeze (usually with a pin or password).

  Equifax Alerts (800) 685-1111 Experian Fraud Center (888) 397-3742 Transunion Fraud Alert (888) 909-8872

- ☐ **Run up-to-date virus scan software** to check for potentially malicious software installed by the scammers. Consider having your computer professionally cleaned.

- ☐ **Change all passwords** if the scammer had access to your device, or if you clicked a malicious link. Especially consider changing your email password and turning on multi-factor authentication.

- ☐ **Report the crime** https://www.usa.gov/where-report-scams will help you determine where you should report the crime.

Continue to monitor all accounts and **expect additional attempts at contact**. The scammers often share their victim database information. **Keep a record of all communication** with scammers.

https://consumer.ftc.gov/articles/what-do-if-you-were-scammed - The FTC walks victims through a variety of scam scenarios, and points to the right resources to report and resolve crime.

https://www.usa.gov/where-report-scams - USA.gov created an interactive quiz to help guide victims to the right place to report various types of scams

https://consumer.ftc.gov/identity-theft-and-online-security - The FTC's user guides and articles about identify theft and online security.

https://www.justice.gov/elderjustice - This is an initiative through the Department of Justice whose mission is to combat elder abuse, neglect, and financial fraud and scams that target older adults.

https://www.ic3.gov/Home/ComplaintChoice - The Internet Crime Complaint Center (IC3) is part of Federal Bureau of Investigation and you can report several different types of cyber crime here

https://www.cisa.gov/report - The Cybersecurity Awareness Program is a national public effort aimed at increasing the understanding of cyber threats.