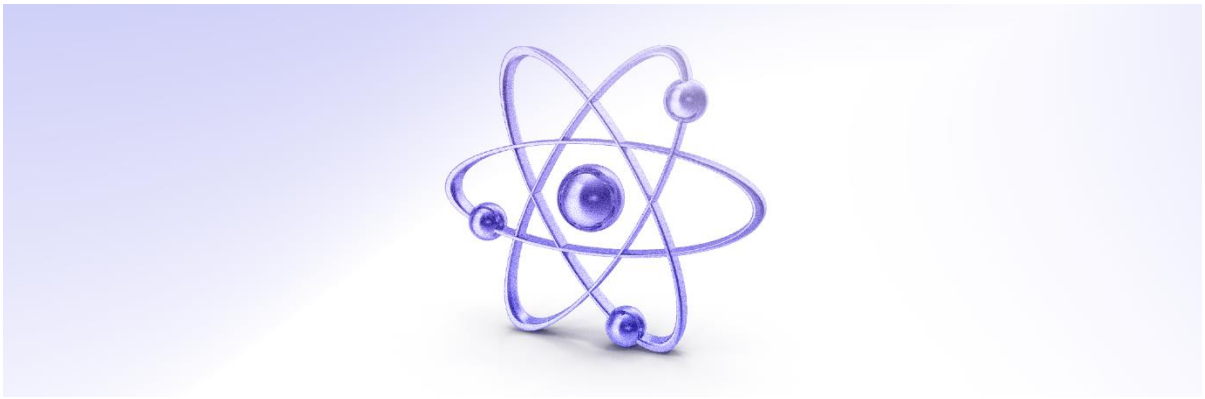
FS-ISAC | Security Tips Newsletter

4 October 2024 | Issue No. 14

Security is *Everyone's* Responsibility



Steps to Recover From Identity Theft

Summary

Have you been the victim of identity theft? Did you know the Federal Trade Commission (FTC) received 5.7 million total fraud and identity theft reports, 1.4 million of them identity theft cases? To help reduce the damage identity theft can cause, here are some steps to help you get started.

Step 1: Contact the companies where you know fraud occurred.

- Contact your bank and companies where the fraud occurred. Explain that someone stole your identity.
- Ask them to close or freeze your accounts. That way, no one can add new charges unless you agree.
- Change the logins, passwords, and PINs for your accounts.

Step 2: Place a fraud alert and get your credit reports.

When you have a fraud alert on your credit report, a business must verify your identity before it opens a new credit account in your name. A fraud alert lasts one year, but you can renew it. Place the fraud alert even if you've already frozen your accounts. (If you haven't, do that too.)

- Place a free, one-year fraud alert by contacting one of the three credit bureaus listed below. That company must tell the other two.

    - **Experian.com/help** 888-EXPERIAN (888-397-3742)
    - **TransUnion.com/credit-help** (888-909-8872)
    - **Equifax.com/personal/credit-report-services** (800-685-1111)

- Check your credit report for accounts you didn't authorize. To get your credit report, call Annual Credit Report at **877-322-8228**, or go to AnnualCreditReport.com. Federal law gives you the right to get a free copy of your credit report every 12 months from each of the three nationwide credit bureaus. The three bureaus also let you check your credit report once a week for free at AnnualCreditReport.com. Review your reports and look for accounts or transactions you don't recognize.

Step 3: Report identity theft to the FTC.

You'll get a free personal recovery plan with the next steps:

- To report in English, go to IdentityTheft.gov
- To report in Spanish, go to RobodeIdentidad.gov
- To make a report in another language, call 877-438-4338 and press 3 to report in your preferred language. Interpreters are available from 9:00 AM – 5:00 PM ET.

Tips to Help You Remain on Guard

- Don't reveal personal or financial information in a text or email, and don't respond to email solicitations for this information.
- Don't click on links sent in a text or email – you might wind up in a scam site built by a cybercriminal.
- Don't send sensitive information over the internet without checking the website's security. Look for URLs that begin with "https" – the 's' stands for secure – rather than "http." A website safety checker like Google Safe Browsing helps, too.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov and the police, and file a report with the Federal Trade Commission.

Getting Help

If you identify suspicious activity involving your institution, contact them immediately.

TLP WHITE

12120 Sunset Hills Rd, Reston
VA 20190