OUCH! February 2024

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for You

Identity Theft: Preventing, Detecting, and Responding

Overview

In today's digital age, your personal information is more valuable than ever. Unfortunately, this also makes it a prime target for identity theft. Understanding this threat, detecting it, and knowing how to protect yourself are essential elements in safeguarding your online digital life.

What is Identity Theft?

Identity theft occurs when someone unlawfully obtains your personal information – your name, identification numbers like your Social Security or passport number, or credit card details, for example – to commit fraud or other crimes. A common form of identity theft is Financial Identity Theft, where someone uses your information for financial fraud. For example, they steal your identity and get a credit card, mortgage or car loan in your name, and you have to pay the bills. However, other types of identity theft exist One example is Medical Identity Theft, where someone steals your medical information and charges medical insurance in your name for medical procedures you never received. Another is Tax-Related Identity Theft, when a criminal uses your tax identification number to file a tax return in your name and claim a fraudulent refund. Then when you attempt to file for a tax return, you cannot get your money back as it's already been submitted to someone else.

Preventive Measures

What can you do to protect yourself? Unfortunately, it is not as easy as it sounds, as so many organizations already have your information and it's up to them to protect it. However, there are some key steps you can take.

- **Strong Passwords**: One of the most effective ways to protect yourself is secure each of your accounts with a unique, long password, and when possible, enable multi-factor authentication.
- **Regular Software Updates**: Ensure your devices are updated with the latest security patches and features by enabling automatic updating on all your devices.
- **Credit Cards**: Use credit cards for online purchases, never debit cards, as credit cards give you far more protection against fraud. Another idea is to use one credit card for just online purchases and another for in-person purchases. Some services provide virtual or one-time use credit cards for every online purchase.
- **Credit Freeze:** A credit freeze locks your credit report, preventing fraudsters from opening new accounts in your name. This can be done for free by contacting the major credit bureaus. This may not be an option in all countries.

Detecting Identity Theft

Early detection is one of the most powerful ways you can protect yourself. The sooner you detect your identity is being used by someone else, the sooner you can act. Some of the most common indications of identity theft include:

- **Unusual Financial Statements:** Regularly monitor all your bank and credit card statements. You want to look for any charges or money transfers you know you did not make. A great way to do this is to enable automatic notifications. This way anytime there is a charge to your credit card or a change to your savings or checking account you are notified right away.
- **Irregular Credit Reports**: Annually review your credit reports for suspicious activity. You are looking for any new loans in your name that you know you did not make or any major changes in your credit rating.
- **Mysterious Bills or Notifications**: Be wary if you begin receiving bills for items you know you never purchased, or if you are contacted by payment agencies for unpaid bills for items or services you never purchased.
- **Unexpected Denials**: If you're unexpectedly denied your tax refund, or a credit or a loan application, investigate why.

Responding to and Recovering from Identity Theft

If you are concerned that your identity has been compromised, act right away.

- **Report Immediately**: Report right away if you suspect an incident. For example, if you identify fraudulent activity in your bank account or credit card, contact your bank. Also, file a report with local law enforcement. This can be crucial in proving the crime and helping you recover any costs or file insurance claims.
- **Fraud Alerts and Credit Freezes**: Place a fraud alert on your credit reports and consider a credit freeze if you have not already. In addition, work with credit bureaus to remove fraudulent information.
- **Document Everything**: When calling organizations to recover, be sure to keep detailed records of your communications and actions taken, to include who you talked to, what date / time, and what was discussed.
- **Change Passwords**: Update passwords for all your key accounts. If you do not have a password manager to track all your new passwords, consider getting one.

Conclusion

By understanding what identity theft is and employing these measures, you can greatly reduce your risk of becoming a victim.

Resources

Password Managers: https://www.sans.org/newsletters/ouch/power-password-managers/
Securing Your Financial Accounts: https://www.sans.org/newsletters/ouch/securing-financial-accounts/
Credit Freezes: https://www.usa.gov/credit
Report Identity Theft: https://identitytheft.org