FinStart

What you can do to reduce the risk of fraud

If enough of your personal information is stolen, someone may be able to impersonate you and withdraw money from your accounts or borrow money in your name.

Know what's going on in your accounts

1. Monitor all your accounts regularly for unusual activity and e-transfers you haven't authorized. Call your bank if anything looks suspicious.
2. If one of your accounts is breached, review activity across all accounts and change passwords.
3. It's also worth checking your credit history as it should record any unauthorized activity in your accounts. Look for any new loans or mortgages set up in your name, and review inquiries into your credit report that you have not requested.
    - Equifax and TransUnion, two main companies that maintain credit histories, offer free access to your credit report online.
    - You may also be able to get access to your credit reports via your bank. With some banks you may be able to set up alerts for changes in your credit report.
4. Ask your bank what other monitoring tools it offers. For example, you can set up email alerts on your accounts to monitor if they are accessed from a different phone or computer than usual.

Mind your passwords and PINs

5. Be discreet with your PIN / login details at ATMs or debit/credit card terminals in public places.
6. Don't save your card numbers / passwords. If your device is lost, there's no way to unsave it.
7. Watch for emails meant to con you into providing a login and password to your accounts.
8. Use two-factor authentication (like a PIN and one other).
9. Sign the back of your bank and credit cards.
10. Consider using a different PIN, login, password, and security questions for each account.
11. Consider changing passwords regularly.
12. Make strong passwords.
    - A good starting point is a combination of letters – small and large cap, numbers, and special characters that does not use your name or account number.
    - If offered, follow your bank's online system suggestions on what makes a strong password.

Other ideas

13. Log into your bank's website directly - don't click links in emails.
14. Always sign off your online banking or mobile app after you finish.
15. Don't send confidential information by email over the Internet.
16. Install up-to-date antivirus program and other security on the devices that you use for your online banking and investing, and tap-and-go payments with our smartphone.
17. Consider doing financial transactions on only one or two devices (your personal computer and phone). Don't do financial transactions on a public WiFi network.
18. Beware of electronic pick-pockets when you use contactless (tap) credit and debit cards. They can read most of the data on the card, except the three digits on the back next to your signature. Consider using protective shields.