IDENTITY THEFT

"Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity" - Wikipedia

BE CAREFUL

While there are many ways for your identity to get stolen, the easiest way to become a victim of identity theft is by sharing personal information over the internet. If you aren't careful, criminals could steal your identity by finding any of the following:

Social Security Number

Credit Card Information

Bank Account Number

Personal Identification

(driver's license, passport, etc.)

Stolen Passwords

PROTECT YOURSELF

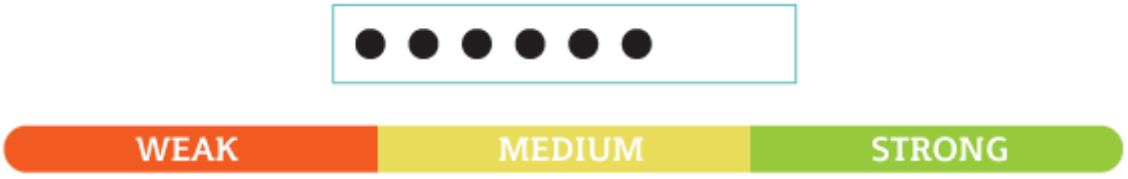
The best way to make sure that your identity never gets stolen is to act right now and follow these steps to protect yourself before an identity theft attacks.

PASSWORDS

Your password's job is to protect almost everything on your computer; this includes your personal information, important files, and items with sentimental value.

Creating a strong password is an easy step that goes a long way. The lock on your front door is a complicated system of tumblers that isn't easily opened without a key. Like the lock,

your password should seem complicated to others but simple to you.



Following these steps will help you easily create a strong password:

Use more than one password.

Using the same password for multiple accounts is an easy way to lose everything you have. Use different passwords so that if one account is broken into, the others will stay safe.

Be Relevant and Irrelevant.

Make a password that you will recognize, but to others it seems random. Never use information that can be directly related to you in your password; like your name, social security number, address, etc.

Use (not-so) random characters.

A password that looks random to the naked eye is more than perfect. For example: MFCIB93 seems like a bunch of gibberish but is easily translated into: My Favorite Color Is Blue and the numbers could refer to anything, like your birth year.

Length is important.

The longer your password is, the harder to figure out what it is. This is the reason for a minimum character length on most websites that you have accounts on.

Use the SUPR test.

Strong Is the password strong? (make sure it's long and looks like random letters and numbers).

Unique Is the password unrelated to your other passwords?

Practical Can you remember it without having to write it down?

Recent Have you changed it recently?

CREDIT REPORT

Your credit report is an archive of all of your credit transactions. Reviewing it every now and then is an easy way to make sure there aren't any accounts or transactions that you are unaware of.

If you are suspicious of an identity thief using your account, you can put a fraud alert on your credit report by contacting one of these three credit reporting companies (U.S. residents only).

Equifax: 1-800-525-6285

Experian: 1-800-397-3742

TransUnion: 1-800-680-7289

SAVING YOUR IDENTITY

The fraud alert will make it hard for any identity theft to make any more transactions using your information. The alert lasts for at least 90 days and if need be, you can create an Identity Theft Report.

IDENTITY THEFT REPORT

An Identity Theft Report helps you fix any false accounts or transactions an identity thief might have made in your name. It will let credit card companies, debt collectors, and businesses know that recent

purchases on your credit report were made by someone other than yourself.

Some things that an Identity Theft Report is used for would be:

Stop Debt Companies

from trying to collect on fraudulent transactions.

Remove

false accounts and transactions made from your credit report.

Extend

the fraud alert on your account.

Examine

your report to discover more about the identity thief.

CREATING AN IDENTITY THEFT REPORT

(IN THE U.S.)

1

Submit an identity theft complaint to the FTC (Federal Trade Commission).

• To do so visit, http://ftc.gov/idtheft

• Or call 1-877-438-4338

2

Make sure to print a copy of your FTC Affidavit. This shows all of the details pertaining to your complaint and you will need a hard copy of it later. You can find the FTC Affidavit on the website above or, if you

called the phone number, you can ask the FTC representative how to get a copy of it.

3

Bring the FTC Affidavit to your local police station and file a police report. Don't forget to get a copy of the police report or the police report number. The FTC Affidavit and the police report together make up your Identity Theft Report.

4

Send a copy of your Identity Theft Report to the companies where you filed for fraud. Now you can ask them to correct all of the false information found under your account.

APPLICATION FOR A COMMONWEALTH VICTIMS' CERTIFICATE (IN AUSTRALIA)

If you are a citizen of Australia and become a victim of identity theft, you will need to fill out a Commonwealth Victims' Certificate, which can be found here:

Commonwealth Victims' Certificate

PHISHING

Click here to verify and update your information

While there are many online scams on the internet, phishing is one that is geared specifically toward retrieving someone's personal information and using it to harm them. An identity thief, known as the phisher, will lure victims using emails and websites that seem harmless or secure.

YOU'VE BEEN SCAMMED!!!*

Be careful when providing any personal information online.

*You haven't. But you're lucky this time!

Some common phishing messages would be:

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

FAKE EMAILS

YOU'VE WON!!! Redeem your prize before it's too late!

Be on the lookout for suspicious looking emails. They will usually contain urgent requests for your personal information.

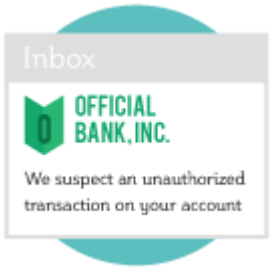
SCAMMED AGAIN!!!*

Stay away from any phishy looking emails!

*No actual scams here, but be careful!

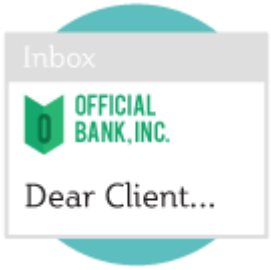
These steps will help you weed out emails that might try to steal your information:

Phisher emails will typically ask for information such as usernames, passwords, credit card numbers, social security numbers, date of birth, etc.



The emails will try to look official, replicating a bank or organization. Look for a digital signature if you are unsure if the email is real.

Phishers try to get people to react immediately, so lure emails generally have upsetting or exciting, but false, statements



Phisher emails usually aren't personalized, meaning they generally don't contain your name or other information. It's possible that they can be personalized, though, so if you are unsure of any email make sure to call the bank or company to be sure.

AVOID A PHISHING ATTACK

Some easy ways to make sure you are never a victim to phishing are:

Avoid filling out the information that the email asks you to give. Only give personal information through a secure website or over the phone.

Never use the links in the email, instant message, or wherever you suspect someone might be trying to steal your information.

Review your credit card and bank statements to make sure all of your personal information is correct. (Address, phone number, date of birth, etc.)

Beware of false websites. Phishers are able to "spoof," or forge, a site into looking like a legitimate address.

> They can make the site look secure, including the "s" in https: at the beginning of the web address.

Phishers can also fake the yellow lock found at the top of some secure web pages.

Check to make sure you're on the right website. Just because the page looks familiar doesn't mean it's real.

Good Address:

(Example) www.paypal.com/login.htm

Bad Address:

(Example) www.yougotscammed.com/paypal/login.htm