Cyber Security Awareness

SLC CYBER Security: Identity Theft

What is Identity Theft?

There are a number of different types of identity theft, but the key point is the use of another person's personal information typically for financial gains. This could be stealing money from someone's bank accounts, or opening bank accounts and credit cards under their name, changing passwords for online accounts, or even so far as renting and buying homes in the name of the person. A high profile case of identity theft is the Wells Fargo scandal. This involved over 1.5 million fake accounts being opened that may not have been authorized. (Egan, 2016) This involved roughly 560,000 credit card applications and $400.000 in fees incurred.

Why should you be worried?

You might be thinking why should I worry about this? This happens to other people… but does it really? Canadian Anti-Fraud Center (2015) reports that the number of victims of identity theft has continued to increase since 2012. In 2014, there were over 20,000 reports of identity theft in Canada.

CYBER Security: Identity Theft

7 Tips to Avoid Becoming a Victim of Identity Theft

1. **Don't give out sensitive information!** Banks and government institutions will never ask for your account number, social insurance number or other sensitive information over the internet. Many scams use a scare tactic to create a sense of urgency that forces you to act before thinking – Credible institutions will never use scare tactics, so when receiving these emails, assess its credibility and delete the email if you believe it could be fishy.

2. **Review your bank statements often –** The number one driver of identity theft is financial gain! Many identity thieves and scams target personal information to gain accesses to your bank account. To ensure that there are no unexplainable transactions or theft goes unnoticed, we suggest that you review statements monthly. This will give you ample time to report any signs of identity – making sure your hard earned money stays safe.

3. **Shred sensitive documents before placing them in the recycle –** Now I know you're thinking this may be overboard, but really you never know who may be able to see this information once the recycle has been taken out, to help eliminate personal information being seen, shed it. This includes removing labels from prescription bottles, bank statements, and anything else that has account numbers, addresses, and other private information. This private information can be used to piece together account information that could lead to identity theft!
4. **Computer safety is key!** Keep your computer up-to-date and make sure you have anti-virus software. Avoid doing banking on public Wi-Fi, and don't share password. To learn more about password security, check our blog from September!
5. **Only use safe sites for on-line shopping** - Look for the "verified signing" or "safe and secure" icons when making online payments. If possible, ship to a local store instead of your home address. If using mobile device, use the app as it is typically more secure.

6. **Be careful with your credit and debit cards -** Don't leave your credit card or debit card out in public or let others use them, even if you are only with bff's! Be leery of people around you when using ATMs or paying in stores. When you activate a new card, shred the old one.
7. **Check credit rating approximately once a year** - Don't check your rating more often than needed, but check it when applying for a credit card, loan, or any other time when needed. Avoid checking more than once a year unless necessary. Be aware of how to properly close a credit card and how to remove credit cards that have never been active.

Now that you're an expert in Identity Theft… SHOUT OUT TO US! Let us know your top tips to protect yourself by tweeting us or mentioning us on FB!

For more topics on e-security click here.

Got a great idea for next month's **SLC CYBER Security –** timely information, you need to know. Share it! Let us know here or tweet us using #SLCE-security