SWC Safety Moment – September / October 2020

By DCC Hans Uhr

"FRAUD & PASSWORD"

Hi Everyone

I hope you and your family is healthy and you are able to keep up with the daily challenges and the neever ending chanches. School has started again and while it feels like a roller coaster, its at least a step more going back to “normal”.

It’s a while since our last safety moment but there is only so much you can talk about internet safety and protocols and after that its getting to repetitive. We had to take it day by day and follow the directive from all governement levels.

While there is no safety tips or safety report from Scouts Canada I have noticed that fraud, spam, phissing and hacking has become a pandemic in its self.

Some classics:

- Call from tax department that you are under investigation.
  (This is usualy an automated phone call requesting you to push #1)

- E-Mail that promisses you a lots of money of you help them with a money transfer.
  (Usualy someone died or is sick and needs to transfer a large amount of money with your help)

- E-mail that requests you to go and buy some gift cards.
  (Ireceived an email from my boss to go and by gift cards sinece he was in a meeting. I checked and he was realy in a meeting. I didn’t do it but a bit later and other person fell for the trap and lost $3600)

- E-mail that ask for additional personal information e.g. credit card, account number.

- E-mail that ask you to claim a reward.
  (Promissing you gifts, vacation, cash prices, etc. Often received afetr you go shopping or buy from the internet.)

- Amazon, etc. is asking to confirm your info and credit card number.
  (You may receive and e-mail from a webpage that looks identical to Amazon webpage and they will ask you to confirm your order by providing your info and credit card number.)

Ther are many more. Some are very old frauds but unfortenetly people are still falling for. Others are new, very smart designed and many people fall into the trap.

Your only protection is your senses and a strong password. **Do not open or click on links you don't know**. Please confirm that the e-mail or the call is ligimit.

If its sound to good please be extra careful, keep in you mind that nothing is for free.

They are not always after your money but rather your identity. With your identity stolen, they can achive much more then just take a few dollars from you and they virtuly can destroy your life. I almost lost my house because of identity theft.

Password

Consider to have a strong password or password phrase for each of your accounts. If you have a weak password, it is possible to link it to your other accounts or divices and hack into your information.
It is amazing that people still use 12345, 123ABC, birth dated, anniversary dates, etc.
By the way if you use any of this passwords, you may loose your protection if you have a fraud claim on your credit card, bank account, etc.

I have attached some tips and information from RCMP and advisors for your concideration. I also have attached a link to the RCMP webpage, they have many useful information.

https://www.rcmp-grc.gc.ca/to-ot/tis-set/cyber-tips-conseils-eng.htm

If you have any questions, concerns or of you would like to address a curtain topic, please let myself, any one of the support scouters or one of the CK3's know,

Thank you and stay safe
Hans Uhr, DCC Safety, Shining Water Council
uhr.hans@gmail.com / hans.uhr@scouts.ca / 905-806-7344

RCMP - Tips

1. **Use Strong Passwords**
   Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. **Secure your computer**
   - **Activate your firewall**
     Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
   - **Use anti-virus/malware software**
     Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
   - **Block spyware attacks**
     Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.
3. **Be Social-Media Savvy**
   Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!
4. **Secure your Mobile Devices**
   Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

5. **Install the latest operating system updates**
   Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.
6. **Protect your Data**
   Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.
7. **Secure your wireless network**
   Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.
8. **Protect your e-identity**
   Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you've enabled privacy settings (e.g. when accessing/using social networking sites).
9. **Avoid being scammed**
   Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.
10. **Call the right person for help**
    Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

For more information on helping children protect themselves while on the Internet, visit: Cybertip.ca.
For more information on Cyber Security, visit: Get Cyber Safe
For more information about online fraud, scams or identity theft, visit:

- Scams and Fraud