fairfirst INSURANCE
A FAIRFAX Company

CYBERSECURITY FOR INDIVIDUALS

V 1.0 12/06/2020

When countries were put on lockdown due to the COVID-19 outbreak, many of our daily routines such as shopping, working, education were shifted to the online space. Even though this was the sensible choice, this new normal has dawned a new set of challenges.

As people spend more time online, cybercriminals became more active, posing a serious threat to your privacy and devices. Whether it's hacking into your office network to compromise confidential data, planting spyware or hacking into your bank accounts, cybercriminals have left thousands of victims affected worldwide.

With the chance for such threats increasing, this guideline will help secure your digital presence while protecting yourself from possible attacks through any of your devices.

ONLINE SHOPPING

How do attackers target online shoppers?

It’s extremely important to take extra precautions to ensure your personal information is kept safe and out of the hands of the wrong people. There are several things you should keep in mind when making online transactions to guarantee your security.

There are three common ways that attackers can take advantage of online shoppers:

01 Creating fraudulent sites and e-mail messages:

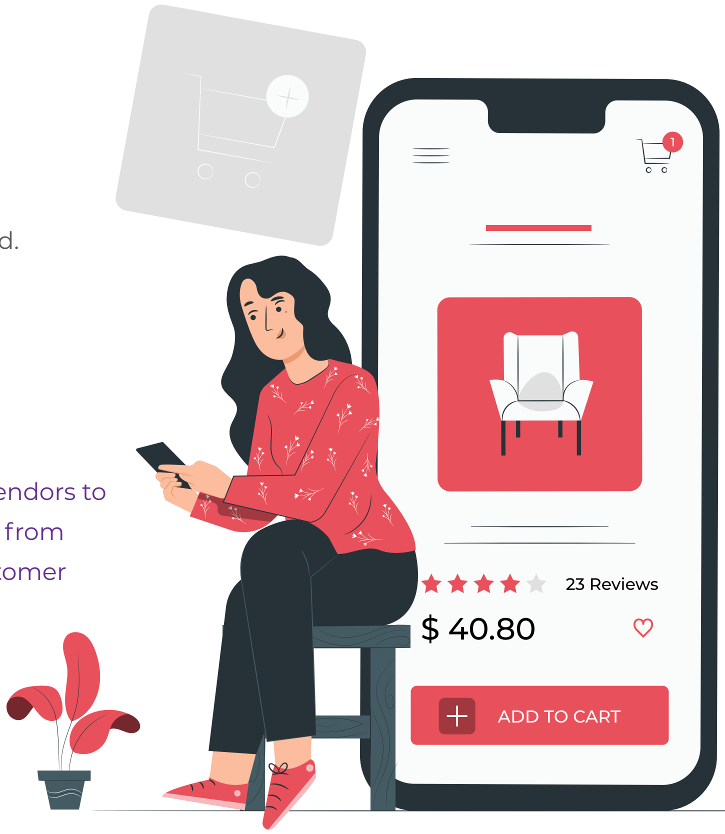
- In the real world when you visit a supermarket, you know exactly where you are and how genuine the seller is. But in an online shopping environment, you may be unaware that you have reached a fake website.
- Attackers can create malicious websites or e-mail messages that appear to be legitimate or they may pretend by appearing as charities, reputed organizations etc.
- Especially after natural disasters or during holiday seasons, attackers create malicious sites and e-mail messages trying to convince you on buying stuff, providing free delivery, supporting charity funds etc.

02 Intercepting insecure transactions:

- If a vendor does not use encryption, your information may be intercepted as and when it is transmitted.

03 Targeting vulnerable computers:

- If your computer is unprotected from viruses or other malicious codes, an attacker may be able to gain access to your computer and all of the information on it.
- It is also important for vendors to protect their computers from attackers accessing customer databases.



HOW CAN YOU PROTECT YOURSELF?

- Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor. Some attackers may try to trick you by creating malicious websites that appear to be legitimate, so you should verify the legitimacy before supplying any information.

- Locate and note phone numbers and physical addresses of vendors in case there is a problem with your transaction or your bill.

- Make sure your information is being encrypted. Also, try to learn how to use the information in the address bar and its proximity. e.g. padlock, i-Information etc.

Click on the padlock icon to the right or left of the website's address and then click the "View Certificate" link. The Certificate dialog box will open. Information about the SSL certificate appears immediately.

- Be wary of e-mails requesting information – attackers may attempt to gather information by sending e-mails requesting that you confirm purchases or account information. Legitimate businesses will not solicit this type of information through e-mail. Do not provide sensitive information through e-mail. If you receive an unsolicited e-mail from a business, instead of clicking on the provided link, directly log on to the authentic website by typing the address yourself.

- You can minimize potential damage by using a single, low-limit credit card to make all of your online purchases. Credit cards are always going to give you more protection than a debit card. Reputable sites will accept a variety of credit cards, while suspicious sites may ask for your credit/debit card numbers for validation.

- Check your shopping app settings – look for apps that tell you what they do with your data and how they keep it secure.

- Check your statements – keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements. If there is a discrepancy, report it immediately.

AVOIDING BEING A VICTIM OF A PHISHING ATTACK

In today's busy world with the new normal environment and virtual activities taking precedence, people sometimes consider loosely on certain e-mails and requests. So they fall into trouble and become a victim of a phishing attack, thus exposing important information.

Identifying phishing attempts:

- **E-mails with suspicious sender's address**
  The sender's address may look like that of a legitimate business. Cybercriminals often use an e-mail address that closely resembles one from a reputable company by altering or omitting a few characters.

- **Generic greetings and signature**
  Both a generic greeting such as "Dear Valued Customer" or "Sir/Madam" and a lack of contact information in the signature block are strong indicators of a phishing e-mail. A trusted organization will normally address you by name and provide their contact information.

- **Spoofed hyperlinks and websites**
  If you hover your cursor over any links in the body of the e-mail, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain.

- **Spelling and layout**
  Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.

- **Suspicious attachments**
  An unsolicited e-mail requesting a user to download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

CHILDREN IN CYBERSPACE

The internet has opened a new world for children to explore and learn. And they are the fastest growing users of the Internet. This has its pros and cons. But as parents you always need to be vigilant about the many dangers this access poses for your children. It's important to teach them how to get the most out of these technologies while keeping them safe.

Unique risks that are associated with children:

- When children are using your computer, there are unique risks associated which cannot be managed by the system itself.
- This is because children are innocent, curious and have a desire to be independent, and are therefore afraid of getting punished for doing something unknowingly.
- While the child is attending an online class, researching for information or doing a test paper, they may sometimes unintentionally visit a malicious web page. As a result, your machine could get infected with a virus. Fearing the punishment the child may not tell you what happened.
- Children might become prey to predators who launch phishing attacks. They trust misrepresented e-mails or anonymous messages sent by them.
- Another growing problem is cyberbullying. These threats are even greater if a child has access to e-mail or instant messaging apps, visits chat rooms, and/or uses social networking sites.

The duty of parents:

- **Make sure that the software is updated**
  Make sure your child's machine has the latest update of security patches and an updated virus guard.
- **Parents should be involved with their children**
  When children are on the computer searching a topic, playing games or attending to school work, parents should support and be involved with their work in a friendly manner. This will allow them to supervise the child's online activities while teaching them good computer habits.
- **Keep the computer in an open area**
  Parents should be able to easily monitor what their children are doing. If the child is doing something which they are normally not supposed to do, the parents can intervene early and avoid any negative consequences.

Set rules and warn about dangers

Make sure your child knows the boundaries of what they are allowed to do on the computer. These boundaries should be appropriate for the child's age, knowledge, and maturity, but they may include rules about how long they are allowed to be on the computer, what sites they are allowed to visit, what software programs they can use, and what tasks or activities they are allowed to do. You should also talk to children about the dangers of the internet so that they recognize any suspicious behaviour or activity.

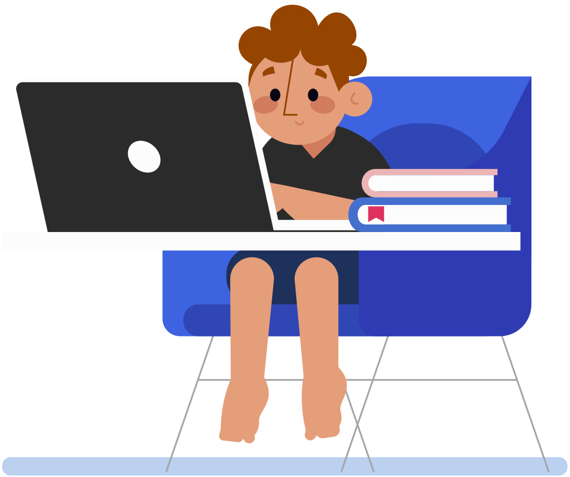
- **Monitor computer activity**
  Be aware of what your child is doing on the computer, including which websites they are visiting. If they are using e-mail, instant messaging, or chat rooms, try to get a sense of who they are corresponding with and whether they actually know them.

- **Let your child know you can talk to them easily**
  Let your child know that they can approach you with any questions or concerns about certain behaviours or problems they may have encountered on the computer in a judgement-free environment.

- **Let your child have a separate account**
  Most operating systems give you the option of creating a different user account for each user. If you're worried that your child may accidentally access, modify, and/or delete your files, you can give them a separate account and decrease the amount of access and number of privileges they have.

- **Consider implementing parental controls**
  Set some parental controls within your browser. For example, Internet Explorer allows you to restrict or allow certain websites to be viewed on your computer, and you can protect these settings with a password. To find those options, click 'Tools' on your menu bar, select 'Internet Options', choose the 'Content' tab and click the 'Enable' button under 'Content Advisor'.

- **Try to use available support services from your ISP**
  Some ISPs offer services designed to protect children online. Contact your ISP to see if any of these services are available through them.



Disclaimer: The guidelines outlined in this document are meant to safeguard you and your loved ones from Cyber threats. Seek professional advice if you wish to clarify any section of this document or take any action based on this document.

This document has been developed based on the information published by the US Department of Homeland Security and in consultation with the IT Department of Fairfirst Insurance.