Five ways to protect your family online

By Carey Van Vaanderen

15 Apr 2014

Whilst we all go about our lives aware of external danger and ensuring the best security to keep such danger at bay, we can be apathetic about the threats that lurk online.

Teach your children safe social networking. (Image: Kevit Dilmen, via Wikimedia Commons)

Children do not realise the potential risks of the internet and perhaps do neither one's in-laws or grandparents, who naively go about opening links that are potentially harmful. Cyber-attacks can be inconvenient but they can also have results that are far more dangerous, such an attack can mean financial loss and reputation damage.

Safety online tips for families

Here are some tips that you can use to ensure that you and your family are safe whilst online.

1. Secure your home Wi-Fi Network - think of your home Wi-Fi network as your front door. It is essential you have a lock on both to ensure safety and security. Neglecting to secure your Wi-Fi means that someone is able to intercept data that is being sent or received.

Neighbours, or people nearby, are able to use the network to access the internet, which may slow down activities or consume all your data. Securing your network is the first step to keeping your information safe.

2. Teach your children safe social networking - online risks that your children face increase as they get older. Children become more involved with social networks, they use the internet on a more regular basis and they grow more curious. Start your education by teaching your child these simple facts:
• Nothing on the internet is 100% private
• Everything shared on the internet is forever, don't say or share something that will put you in a compromising position

later on.
• Privacy matters, over-sharing online can be detrimental, especially when you are sharing private information.
• Let your child know that it is never ever okay to provide information to anyone on the internet without approval.

3. Ensure safe browsing - most social sites are designed for age groups of thirteen and older. However, even if a child is of age, parents should monitor their child's account use. Parents can set up privacy settings and control whom their child can or cannot befriend. Do not allow your child to share any contact details, such as telephone number, in their profile set up. Remember, discuss the potential dangers of social networks and ensure that a child is well educated on what to watch out for and avoid.

4. Learn how to avoid phishing attacks - phishing attacks are typically fraudulent emails that appear to come from legitimate enterprises. Often you are taken to a bogus website, and you are then asked to divulge sensitive information such as passwords, credit card details, or other account information. There are various types of phishing. Spear phishing is directed at specific individuals. They are pointed and attackers go to great lengths to make the attack look believable to increase the likelihood of success:
• Your bank will never ask you to send your password or personal information by mail.
• Never go to your bank's website by clicking on the links included in emails
• Enhance the security of your computer
• Enter sensitive information in secure websites only
• Keep up to date on all the latest in phishing scams

5. Have a complete internet security solution - make sure that your computer has a proactive security system that keeps you and your family safe from malware. The security should offer you a complete solution against all types of infiltration and attacks. Such solutions can offer you peace of mind with features such as antivirus, parental control, anti-phishing, device control and more.

ABOUT THE AUTHOR

Carey Van Vlaanderen is CEO, ESET Southern Africa.