BIZCOMMUNITY

Social media: Stay safe online

By Carey van Vlaanderen

12 Jun 2014

Social media has more than its fair share of malicious content - here are some tips on how to avoid it, and keep your children out of harm's way.

Social media has become flooded by malicious content, and it is becoming more difficult to discern between what is safe and what is not. Although children may not be the common target of cybercriminals, they do gather online where hackers lay their traps, and a common tactic of cybercriminals is to use events and popular culture as a part of their schemes to lure victims.

Some people expand their social networking connections by accepting every request they receive. Quite simply, if you do not know the person, say no to their request. A way to explain this, especially to the kids, is to ask: Would they invite every one of their social media friends over to their house?

A hidden threat

A common social engineering trick is for a hacker to socially engineer one person's email password and then have access to that person's contact list - and possibly that person's social networking contacts. Another possibility is that a download has malicious software embedded; if you download, you become infected, and the hacker has access to your machine, email account, and social network account.

A threat on your computer can show few if any symptoms and survive for a prolonged period undetected. In general though, criminals are trying to access information that will lead them to money as quickly and easily as possible.

1. Think before you click
Not every link you come across in social media is what it seems; some are scams, or wild or salacious news stories. Teach your child (and yourself) to rather Google the subject of the link or type a websites main URL into a browser instead of clicking the link.

2. Only accept friends you trust enough to invite to dinner
Accepting a friendship from someone they don't know puts your child, and their reputation, potentially at risk. Note: Make sure you understand the social media settings, and ensure that your child's security is on the maximum settings.

3. Strong passwords a must
Strong passwords can go a long way in helping secure information, so choose a password that is 10 characters long and

consists of a combination of letters, number, and special characters. Change your password periodically to reduce the likelihood of it being compromised.

4. Don't share links or posts without checking
Sharing information and links without verifying them is risky. You may be tricked into spreading inappropriate or even malicious content.

5. Say NO to geo-locating
Location services allow teenagers to publicly post their current location, and it is not just their friends who can see where they are. This means that teens could be leaving a trail of where they are. Make sure that you have checked the privacy setting and that geo-location is turned off, when it is off you have to be asked for permission to use your location. This gives more control over the information that is posted as well as information that is collected.

Facebook and Twitter users who want to make sure that they are protected while surfing the website can turn to ESET's free Social Media Scanner, an app that secures the content on their timeline, newsfeed and private messages against cyber threats. If the app (which works in real time) detects anything malicious, it will inform the user via email with instructions on how to clean their profile.

ABOUT CAREY VAN VLAANDEREN

Carey van Vlaanderen is CEO of ESET Southern Africa. ESET is a global provider of security software for enterprises and consumers and is dedicated to delivering instant, comprehensive protection against evolving computer security threats.
- Teens and Instagram: Practical steps parents can take to help teens navigate Instagram safely - 17 Mar 2022
- Social media: Stay safe online - 12 Jun 2014

View my profile and articles...