LUMKA!

OBSERVE.THINK.CLICK | December 2017

The Monthly Cybersecurity Awareness Newsletter

OBSERVE.THINK.CLICK

In this issue

Social Media

Overview

Social media sites, such as Facebook, Twitter, Instagram and LinkedIn, are amazing resources, allowing you to meet, interact and share with people around the world.
However, all this power also brings risk for you, your family, friends and employer.
In this newsletter, we explain what these dangers are and how to use these sites securely and safely.

> Whether it be entertainment, news, education, customer service, or even networking, Social Media is readily used at least once a day by over 40% of South African's, predominantly through mobile phones.

Privacy

A common concern with social media is protecting your personal information. Potential dangers include:
Impacting Your Future: Some organizations search social media sites as part of background checks. Embarrassing or incriminating photos or posts, no matter how old, could prevent you from getting hired or promoted. In addition, many universities conduct similar checks for new student applications. Privacy options may not protect you, as these organizations can ask you to "Like" or join their pages or certain posts may be archived on multiple sites.

Attacks Against You: Cyber attackers can analyze your posts and use them to gain access to your or your organization's information. For example, they can use information you share to guess the answers to the secret questions that reset your online passwords, create targeted email attacks against you (called spearfishing) or call someone in your organization pretending to be you. In addition, these attacks can spill into the physical world, such as identifying where you work or live.

Accidently Harming Your Employer: Criminals or competitors can use any sensitive information you post about your organization against your employer. In addition, your posts can potentially cause reputational harm for your organization. Be sure to check your organization's policies before posting anything about your job. In addition, some of your social media posts may be monitored.

Social Media

Social media sites are fun and powerful, but be careful what you share and with whom.

The best protection is to limit what you post.
Yes, privacy options can provide some protection. However, they are often confusing and change frequently without your knowledge. What you thought was private can quickly become public for various reasons. In addition, the privacy of your posts is only as secure as the people you share them with. The more friends or contacts you share with, the more likely that information will become public. You should assume anything you post can or will become a public and permanent part of the Internet.
Finally, be aware of what friends are posting about you. If they post something you are not comfortable with, ask them to take it down. If they refuse or ignore you, contact the social media site and ask the site to remove the content for you. At the same time, be respectful of what you post about others.

Security

In addition to privacy concerns, here are some steps to help protect your social media accounts and online activities:

Login: Protect each of your accounts with a strong, unique password and do not share them with anyone else. In addition, many social media sites support stronger authentication, such as two-step verification. Always enable these stronger authentication methods whenever possible. Finally, do not use your social media account to log in to other sites; if it gets hacked, then all of your accounts are vulnerable.

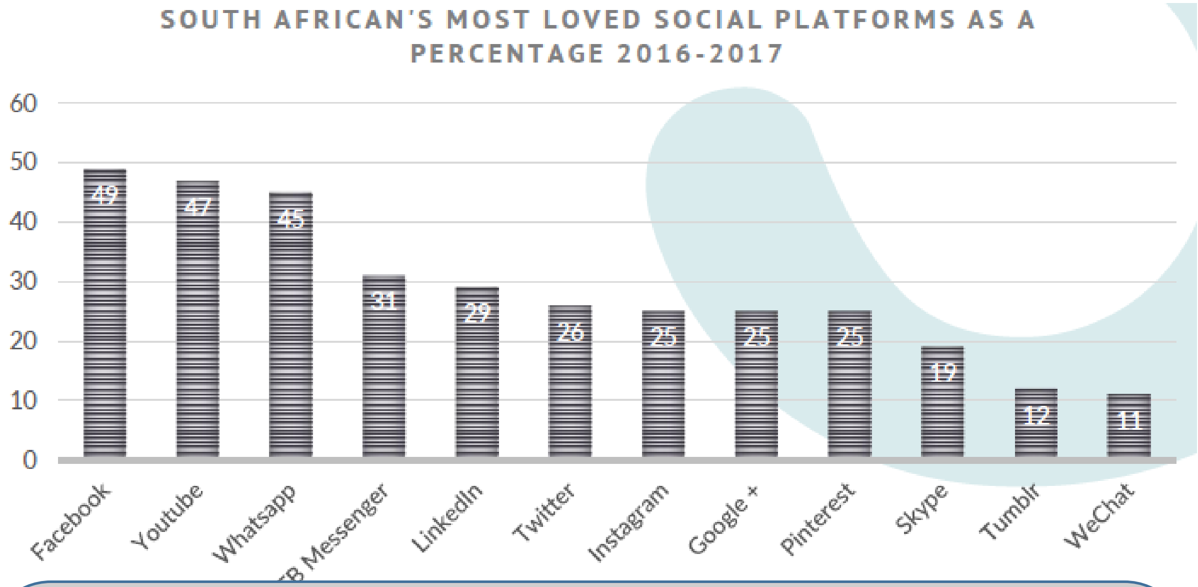
Privacy Settings: If you do use privacy settings, make sure you review and test them regularly. Social media sites often change privacy settings and it is easy to make a mistake. In addition, many apps and services let you tag your location to content that you post (called geotagging). Regularly check these settings if you wish to keep your physical location private.

Encryption: Social media sites use encryption called HTTPS to secure your online connections to the site. Some sites (like Twitter and Google+) enable this by default, while others require you to manually enable HTTPS. Check your social media account settings and enable HTTPS as the default connection whenever possible.

Email: Be suspicious of emails that claim to come from social media sites. These can easily be spoofed attacks sent by cyber criminals. The safest way to reply to such messages is to log in to your social media website directly, perhaps from a saved bookmark, and then read and reply to any messages or notifications from the website.

Malicious Links/Scams: Be cautious of suspicious links or potential scams posted on social media sites. Bad guys use social media to spread their own attacks. Just because a message is posted by a friend does not mean that message is really from them; their account may have been compromised. If a family member or friend has posted an odd message you cannot verify (i.e., they have been robbed and need you to send money), call them on their mobile phone or contact them by some other means to confirm the message is truly from them.

Mobile Apps: Most social media sites provide mobile apps to access your online accounts. Make sure you download these mobile apps from a trusted site and that your smartphone is protected with a strong password. If your smartphone is unlocked when you lose it, anyone can access your social media sites through your smartphone and start posting as you.



Resources

http://qwertydigital.co.za/wp-content/uploads/2017/08/Digital-Statistics-in-South-Africa-2017-Report.pdf

https://www.commonsensemedia.org/social-media
http://www.parenting.com/gallery/social-media-monitoring-kids