OUCH! | March 2018

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for Everyone

Top Tips to Securely Using Social Media

Overview

Social media sites, such as Snapchat, Facebook, Twitter, Instagram, and LinkedIn, are amazing resources, allowing you to meet, interact, and share with people around the world. However, with all this power comes risks--not just for you, but your family, friends, and employer. In this newsletter, we cover the key steps to making the most of social media securely and safely.

Posting

Be careful and think before posting. Anything you post will most likely become public at some point, impacting your reputation and future, including where you can go to school or the jobs you can get. If you don’t want your family or boss to see it, you probably shouldn’t post it. Also, be aware of what others are posting about you. You may have to ask others to remove what they share about you.

Privacy

Almost all social media sites have strong privacy options. Enable them when possible. For example, does the site really need to be able to track your location? In addition, privacy options can be confusing and change often. Make it a habit to check and confirm they are working as you expect them to.

Passphrase

Secure your social media account with a long, unique passphrase. A passphrase is a password made up of multiple words, making it easy for you to type and remember, but hard for cyber attackers to guess.

Lock Down Your Account

Even better, enable two-factor authentication on all of your accounts. This adds a one-time code with your password when you need to log in to your account. This is actually very simple and is one of the most powerful ways to secure your account.

Scams

Just like in email, bad guys will attempt to trick or fool you using social media messages. For example, they may try to trick you out of your password or credit card. Be careful what you click on: if a friend sends you what appears to be an odd message or one that does not sound like them, it could be a cyber attacker pretending to be your friend.

Terms of Services

Know the site's terms of service. Anything you post or upload might become the property of the site.

Work

If you want to post anything about work, check with your supervisor first to make sure it is okay to publicly share.

Follow these tips to enjoy a much safer online experience. To learn more on how to use social media sites safely, or report unauthorized activity, check your social media site's security page.

Subscribe to OUCH! and receive a copy every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Jessica Barker is a world leader in the human side of cyber security. She is the co-founder of Redacted Firm, where she delivers consultancy services to clients across the globe, and is also a well-known speaker. Follow her on twitter at @drjessicabarker.

Resources

Passphrases:	https://www.sans.org/u/B6E
Two-Step Verification:	https://www.sans.org/u/B6J
Securing Today's Online Kids:	https://www.sans.org/u/B6O
Lock Down Your Login:	https://www.lockdownyourlogin.org/

License