September 2017
Volume 12, Issue 09

Staying Secure on Social Media

Enterprise Information Security Program

From the Desk of Ron Jimerson, Chief Information Security Officer

The number of scams and malware taking advantage of social media users and platforms is on the rise. Social media scams are easy to create and can target thousands of people at once due to how users interact with pages, posts, and contacts. Once your account is compromised, malicious actors can leverage it as a conduit to spread scams and malware to your network of friends or contacts. Facebook, Twitter, LinkedIn, and Instagram are a few very common examples of social media sites where you or your account could be at risk. Below we will examine some ways that you can keep your social media accounts more safe through smart online practices.

How to Identify and Prevent Attacks

Shortened URLs are a common tactic used by scammers to conceal where malicious links lead, since many social media sites have a character limit. A simple scam involves an email with links that are allegedly to posts you have been tagged in. The links will use a URL shortening services to hide the true link destination - a malicious site that can infect your device. To avoid this, do not click on shortened links in emails and social media messages you receive. Instead, copy and paste the shortened URL into a URL extender to see where you are really going and then choose to click or not. Additionally, never enter your login credentials in a website that you linked to from a social media post, message, or email. Malicious websites that look like the real thing are often used to steal login credentials to compromise accounts.

Fake coupons are another tactic scammers use commonly on social media platforms. The scammers create a fake coupon requiring you to click a link to download it and put the coupon on a malicious website that can infect your device with malware. Treat these with the same skepticism as other suspicious emails and messages.

Click baiting is another way a scammer can get your information or install malware on your computer. Click baiting is when there is a “teaser” to get you to click on the link. For instance, it might suggest a really interesting story (“you won’t believe what happened next…”), challenge you (“I bet you can’t…),” or promise a “giveaway” or “sweepstake.” With the sweepstakes and giveaways, the scammer creates a fake website giving away a product.

They then post the link on social media, directing users to the website to take part in the giveaway. Once there, you may be prompted to enter information, thus exposing your personal data. The website may alternatively attempt to download malware onto your device.

One way to identify and avoid this type of scam is to look for spelling errors. Another way is to check and see if the website is affiliated with the company purportedly offering the giveaway. Additionally, ask yourself, is the prize too good to be true? Scammers frequently make the prize seemingly larger-than-life in order to attract as many people as possible.

Lastly, when using social media, avoid accepting friend requests from people you do not know. If accepted the scammers can use this to gain access to your personal information with the goal of stealing your identity. If you receive a direct message from someone that you do not trust, delete it. Finally, consider following the guidelines below on what information you should NOT share on social media:

- Your date of birth – this is a piece of personally identifiable information that criminals can use in committing identity theft;
- Your address and phone number – these are privileged pieces of information that you do not need to share on your profile in order to enjoy social media;
- Answers to common "security questions" – if you proudly post pictures of your first new car, your high school sports memorabilia, etc., you are posting the answers to the security questions that are commonly used to validate who you are when accessing sensitive accounts or resetting passwords;
- Location-based check in – these "check-ins" let everyone see that you are not at home and can make you a target!

For more information on social media scams or on securing your social media experience check out:

- https://us.norton.com/yoursecurityresource/detail.jsp?aid=social_media_scams
- https://www.cisecurity.org/white-papers/cis-primer-securing-personal-social-media-accounts/