June 2018

Security Awareness News

the security awareness newsletter for security aware people

ALL ABOUT SOCIAL MEDIA

THE SHADY SIDE OF SOCIAL

PRIVACY IN A SOCIAL WORLD
CONTROLLING WHAT WE LET OTHERS SEE

PASSWORD UNIVERSITY

SELLING YOUR
STUFF ONLINE?

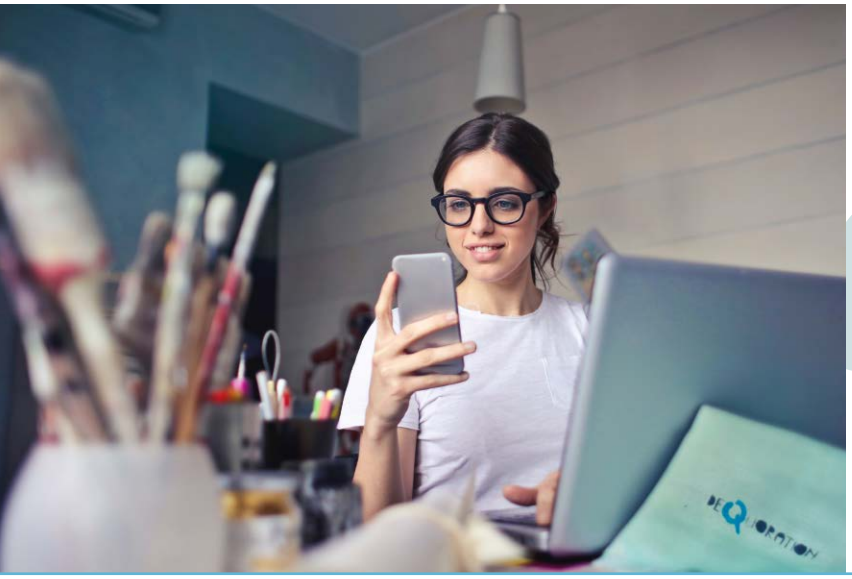
The Shady Side of Social

By the year 2021, the number of social media network users worldwide is expected to surpass 3 billion. That's a lot of people generating content and sharing personal information.

The social media explosion over the last several years has created a cultural phenomenon where seemingly everything is documented. From dating apps to neighborhood watch groups, information has never been more accessible, nor has its life cycle been so infinite. What happens on the internet, stays on the internet.

This accessibility, of course, isn't necessarily a good thing. Scammers now have a huge market to target. Misleading headlines can circulate and distort the accuracy of information. Newsfeeds and timelines provide a massive data stream for phishing attacks and social engineers. And the websites/apps themselves harvest billions of data points about you, your friends, and your family.

At best, social media is a strong tool for communicating and accessing information. At worst, social media represents one of the biggest threats to our privacy (and our sanity). So how do you stay safe in this ever-expanding phenomenon? Only *friend* people you know in real life. Remember that you can't "unshare" something. Consider maxing out your privacy settings. And always follow our organization's policies regarding what is and what is not acceptable to share on social media.



Five Things to Watch For When Socializing Online:

Clickbait Headlines

Unbelievable headlines written with your click in mind can sometimes direct you to dangerous websites or inappropriate material.

Fake Friends

Social engineers impersonate people you know and send you friend requests in hopes of gaining access to private information.

Phishing Attacks

Just like with random links in emails, think before you click on social media platforms, especially when it comes to shortened URLs, which can be used to hide their address.

Like-Farming

A common scam found on Facebook which is known as like-farming, involves fake pages offering bogus promotions or free products in exchange for a like or a share. Once they get enough activity, they often switch the content to feature fraudulent material or they sell the page, along with your info, to other scammers.

Employment Cons

Fraudsters target people looking for jobs by posting malicious ads that say something like "work from home and make a bunch of money!" Never forget that if something sounds too good to be true, it's probably not true.

The social media explosion over the last several years has created a cultural phenomenon where seemingly everything is documented.

PRIVACY IN A SOCIAL WORLD

Controlling What We Let Others See

If there are three words we should all heed when accessing social media, they are "less is more." The less you share, the more control you maintain of your personal information. Never forget that social media sites are in the business of data collection. For all intents and purposes, you are not their customer; you are their product. And they could sell your data to advertisers (who are the actual customers). So, guard your info closely and before posting anything, ask yourself the following questions:

Could this post be used to steal my identity in any way?

Avoid sharing personally identifiable information (PII) both intentionally or accidentally.

Could this post have a negative impact on my personal or professional life?

Remember that tweets and Facebook status updates, etc. exist forever. Even if you delete a post, it's possible someone took a screenshot of it. The internet never forgets.

Will someone consider this post offensive?

The whole idea behind social media is connecting with others. It's certainly more enjoyable to share positive information than divisive or manipulative information.

Does this post inappropriately share info of my friends, family, or co-workers?

It's not just your information you need to protect. Ensure that you are not posting sensitive info of other people, which includes the sharing or tagging a photo of them without their permission.

Is there any chance I will regret posting this?

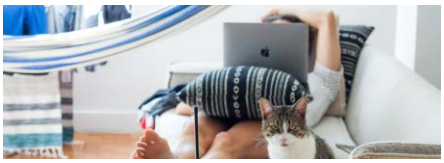
Consider the ramifications of what you share before clicking "post".

Does this violate organizational policy?

Be discreet when posting anything about our organization, clients, and co-workers. Often, it's best to not discuss specific work-related matters or problems on social media!

Social Media and the Workplace

Do you know which sites, if any, you're allowed to visit while at work? Do you know if you're allowed to use social media on work devices? If you're not sure, please ask. Following organizational policies is key to your role as a strong human firewall.



Social Media at Home

Kids will always want to join whatever trendy social media site or app is popular with their friends. So, as parents, we need to set limits on what our kids can access. That means staying up to date on what's out there and regularly reviewing privacy settings. In fact, just as policy helps to guide our behaviors and decisions here at work, a household security policy could help your family! Consider developing a family social media policy to establish which sites are allowed, what info can be shared, and with whom.

Check Your Own Privacy Settings!

When was the last time you modified the privacy settings on your various social network profiles? When was the last time you Googled yourself or checked what others can find about you? When was the last time you cleaned up your "Friends" list to include only those friends you know and truly care to know in real life? It's a good idea to reevaluate your social networking privacy settings from time to time, so you maintain control of your personal posts and data.

Social Media How-Tos: For site-specific information on keeping your accounts safe, check out the following links!

Practice Privacy on Facebook
http://secaware.co/2pU3Ew9

Be More Cyber-Aware on Twitter
http://secaware.co/2qW2am4

Stay Secure on LinkedIn
http://secaware.co/2pCiUzu

PASSWORD UNIVERSITY

The average number of social media accounts held per person has doubled since 2013, from a little over four to nearly eight. And with each new account comes the need for a new username and password. Unfortunately, the temptation to use the same password for each account is too great for many people to ignore.

As you can guess, using the same password for multiple accounts is a major security fail. Why? Because if someone cracks a database containing your password, such as what we saw with the Yahoo data breach, they'll have access to every account associated with that same password. With that in mind, let's review what it means to develop strong, unique passwords.

SNL (Symbols, Numbers, and Letters)

Remember to use symbols, numbers, and letters. Your password should contain all three. And mix up your upper and lowercase letters. This is an easy way to create unique codes.

MFA (Multi-Factor Authentication)

Multiple factors provide extra security. Two-factor authentication, or multi-factor authentication, requires more than just one password to unlock an account. An additional code or pin is also required, and is typically sent to you via email or text. Utilize multiple factors wherever possible.

Password Managers

At home, consider getting a manager. Password managers create, store, and sync your logins and passwords across multiple devices, and can automatically log you into your accounts. With a password manager, many of which are free, the only password you'll ever have to remember again is your master password (which unlocks the password manager giving you access to your accounts).

Are you allowed to use a password manager here at work? Please ask!

Read more: http://secaware.co/2AkAflP

Longer Is Stronger

Most security analysts recommend using a minimum of 12 characters. In fact, passphrases are actually better than passwords. Passphrases incorporate a group of words that form a phrase you can easily remember but is also hard to guess.

Example: AlwaysFollowPolicy2018!!

This passphrase, meant to be an example only, follows the SNL Triad to perfection. It utilizes upper and lowercase, satisfies the minimum character count, and can easily be remembered.

Mobile

Protecting our smartphones, tablets, and laptops with strong passwords is just as important as protecting our bank accounts. Most devices will default to requiring a password. Don't bypass this default setting for any reason, and make sure the code or pattern you choose can't be easily cracked in the event your device is lost or stolen.

Most Important!

Know and follow organizational password and authentication policies. And if you're not sure about something, please ask! There are no stupid questions when it comes to our collective security.

Biometrics

Password alternatives such as fingerprint and retinal scanners are becoming more and more common. Even though they solve certain password issues, like complexity and uniqueness, they also present other privacy concerns. They can't be changed like traditional passwords for obvious reasons. And we should be aware that our fingerprints, and whatever else we use for biometrics, get stored alongside our personal details in massive databases, which can be compromised. Proceed with caution if you choose to use biometrics on your personal devices.

SELLING YOUR STUFF ONLINE?

Social media is a powerful platform for individuals selling things they no longer need. But as always, scammers follow the crowd and target both sellers and buyers. Here are eight ways to avoid getting scammed.

1

Keep all communication on the host site whenever possible.

Some scammers will attempt to deal with you directly through email or text to avoid the security layers of websites like eBay. If you sell to the scammer directly, you have no recourse for action. By staying on-site, you have the ability to file official complaints and potentially get your money back if you make a mistake.

2

Document everything.

Research the buyer before shipping and take screenshots of all conversations. Photograph every angle of your item, especially the packaging if you have to ship your item. Try to think of every possible situation where you might need to show proof that the item is as advertised, and the sale is legitimate.

3

Don't ship your item until funds have cleared.

This one should be obvious, but some scammers will push a sense of urgency and even offer more money if you ship ASAP. As a general rule, never send the buyer your item until payment has cleared.

4

Watch out for fraudulent emails claiming payment has been sent.

Always log directly into your accounts and verify that they have been credited before you ship.

5

Limit the amount of personal info you give out.

Most often, the buyer doesn't need your home address, email address, or even phone number. Only provide the minimum amount of info necessary to complete the transaction.

6

When selling on local market sites (such as Craigslist or Facebook Marketplace), only accept cash.

This is the same concept as not shipping before the funds clear. Remember that once you give a stranger your item, you have no way of getting it back. It's best to demand cash in person. Be sure to count twice, and even though counterfeit money is unlikely, here are eight ways to detect fake bills: **https://secaware.co/2wZ2DvY**.

7

If selling locally, pick a safe place to meet.

Physical safety is more important than avoiding scammers. When selling to a stranger in public, be sure to pick a well-lit, popular location at which to meet the prospective buyer. Even better, find a place that has security cameras such as a bank parking lot. If possible, bring a friend or have them meet you there.

8

Think before you click.

Scammers see public listings as an opportunity to fire off phishing emails. As usual, handle every email with a heavy dose of skepticism.