Big Creek Group
Companies in Touch with Tomorrow

MONTHLY IT NEWSLETTER
JUNE 2022

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.

PRIVACY

Most people would never consider walking into a crowded room and loudly broadcasting to total strangers all the details of their private life--from their health issues to their family and friends' names, ages, jobs, or school locations. But often these same individuals won't think twice about posting that same information on social media. The ramifications of sharing too much can have an impact not only on your personal and professional life but also the lives of your family and friends.

Social media is a great place to reconnect, share, and learn. However, just ensuring that your social media privacy settings are strong isn't the only way to protect yourself. Once you post anything online, you have lost control of it. You need to understand what is being collected and how it is being used. Here are some privacy concerns you should have when using social media:

- **Privacy Settings**: Carefully create and frequently review privacy settings for all of your social media accounts, especially when changes in terms of service and privacy policies take place. Remember that even if you have secured your settings for who can view your postings, all of your information is being collected, mined, and stored on the social media platform servers--perhaps forever.

- **Privacy Tree**: Social media settings can't protect you from friends, relatives, and co-workers who view your postings and then have the ability to share those postings with their circle of friends and so on.
- **Family Sharing**: Everyone loves to talk about their friends and family. But posting silly birthday cake pictures or health and behavior problems can lead to bullying, especially for those who are younger, and could impact their personal lives.
- **Information Sharing**: If a service is "free," then you are the product. Investigations have found that what you are doing online may be sold to others.
- **Location Services**: Check-in data can be added to other personal data to create a profile of your life and habits, which can lead to stalking and open you to other harassing events. In addition, be aware of any location information included in any pictures or videos you post.
- **Artificial Intelligence**: AI, social media, and marketing are the perfect combination. Marketers now use information gathered from your habits online to feed you ads focused on your last search or purchase, and thereby continue to learn even more about you.
- **Digital Death**: When a person dies, their online presence becomes more vulnerable to malicious individuals if their accounts aren't being maintained or eliminated by their survivors. The privacy of an individual is not just about that person alone; it also can impact extended family and friends.
- **Unintentional Disclosure**: The information you post about yourself may reveal much of your personal history, and thus the answers to your online secret security questions.

Privacy is far more than just setting the privacy options in your social media accounts. The more information you share, and the more others share about you, the more information that is collected and used by corporations, governments, and others. One of the best ways to protect yourself is to consider and limit what you share and what others share about you, regardless of the privacy options you use.

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.

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

SECURITY

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.

2FA

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

While social media is a fantastic way to communicate, share, and have fun with others, it is also a low-cost way for cyber criminals to trick and take advantage of millions of people. Don't fall victim to the three most common scams on social media.

Investment Scams

Have you ever seen a post about an investment opportunity that promises a huge return on investment in an extremely quick amount of time with allegedly little to no risk? The reality is, these guarantees are really investment scams. Fraudsters simply steal your money after you pay them. These scams often include ads or success stories from past customers to promote the investments, but those are just fake testimonials to increase your trust. Often these investment scams are about investing in crypto-currencies or real estate, and payment is often made in crypto-currencies or other non-standard payment methods. If an investment seems too good to be true, it most likely is. Remember, there is no such thing as guaranteed, high-return investments. Only invest your money in trusted, well-known resources, not strangers you meet online pushing a get-rich-quick scheme.

Romance Scams

When criminals develop an online relationship with someone they've identified as lonely or vulnerable to trick them out of money, this is known as a romance scam. The criminal will use whatever tactics they can to build trust, including exchanging fake photos or sending gifts, then share a tragic story about needing money to pay for expenses such as hospital bills or for travel costs to visit the victim in person. To avoid actually meeting in person, these criminals may say they work in an industry that prevents them from doing so, such as construction, international medicine, or the military. They often request money as a wire transfer or gift cards to get cash quickly and remain anonymous. These types of scams are not only common on social media but with online dating apps. Be careful with people you meet online, take things slowly, and never send money to someone you have only communicated with online.

Additionally, if you believe someone you know may be vulnerable to such an attack or is in an online relationship that raises these flags, offer to help them. Sometimes it can be very difficult for someone engrossed in an emotional connection to see just how dangerous the situation has become.

Online Shopping Scams

Online shopping scams happen when you purchase items online at extremely low or unbelievable prices but never receive them. Tempting ads on social media will promote incredible prices and have links that take you to sites that appear to be legitimate and sell well-known brands, but these sites are often fake. Be wary of websites that have no contact information, broken contact forms, or use personal email addresses. Type the name of the online store or its web address into a search engine to see what others have said about it. Look for terms like "fraud," "scam," "never again," and "fake." Be very cautious of online promotions or deals that appear too good to be true. It's far safer to purchase items that may cost slightly more, but from trusted sites that you or your friends have used before.

CONCLUSION

Attempts to scam or fool you can happen over almost any form of communication you use--from Skype, WhatsApp, and Slack to Twitter, Facebook, Snapchat, Instagram, and even gaming apps. Communication over these platforms or channels can feel more informal or trustworthy, which is precisely why attackers are using them to fool others. In addition, with today's technologies, it has become much easier for any attacker anywhere in the world to pretend to be anything or anyone they want. It is important to remember that any communications that come your way might not be what they seem and that people are not always who they appear to be.

Here are the most common clues that a message you just received or a post you just read may be an attack:

Urgency: The message has a sense of urgency that demands "immediate action" before something bad happens, like threatening to close your account or send you to jail. The attacker wants to rush you into making a mistake.

Pressure: The message pressures you to bypass or ignore policies or procedures at work.

Curiosity: The message invokes a strong sense of curiosity or promises something that is too good to be true. No, you did not just win the lottery.

Sensitive: The message includes a request for highly sensitive information, such as your credit card number or password, or any information that you're just not comfortable sharing.

Official: The message says it comes from an official organization, but has poor grammar or spelling. Most government organizations will not use social media for official communications directly with you. If you are not sure if the message is legitimate, call the organization back, but use a trusted phone number, such as one from their website.

Impersonation: You receive a message from a friend or co-worker, but the tone or wording just does not sound like them. If you are suspicious, call the sender on the phone to verify they sent the message. It is easy for a cyber attacker to create messages that appear to be from someone you know. In some cases, they can take over one of your friend's accounts and then pretend to be your friend and reach out to you. Be particularly aware of text messages, Twitter, and other short message formats, where it is more difficult to get a sense of the sender's personality.

You are the best defense against scams, cons, and attacks like these. If a post or message seems odd or suspicious, simply ignore or delete it. If it is from someone you personally know, call the person on the phone to confirm if they really sent it. **REMEMBER**: **You** are your own best defense. **You** are in control. Just be on alert for scams like these and you will be able to make the most of social media safely and securely.