Website Security

When was the last time you left your house without locking the doors, turning on the alarm system? Do you have security cameras installed around your home. What about locking your car? Do you have a safe or lockbox for valuables? Times have changed and it is more important than ever to make sure our information is secure. Cybercriminal activity has increased and developed into a highly technical, and successful, problem that must be addressed. Two scenarios to consider:

I received a text informing me that my Netflix account subscription could not be renewed because my payment method was not approved. Two days later, I received another text…same message, different sender. I checked my account and found that my account was not up for renewal. I was being scammed.

One of our own chapter presidents was using Facebook to let their members know when, where, and what time their next meeting would be. In just a few minutes, she received a FB message from a man telling her that he was “impressed” with her and suggested a meeting.

What about your personal information? How many online accounts do you have? How much of your personal information is stored on your computer or smart phone? Ever since the COVID pandemic, we have come to rely on digital communication to contact potential members, employees, or long-lost family. We order clothes, groceries, tools…all kind of items through the internet and pay for them at the same time. We access our health information through online portfolios provided by our medical facilities. All of that information is readily available to us wherever we are, but it is also available to others invading our digital spaces to use for their own desires.

So, what do we do about it? The number one suggestion I have for you today is to stop being so trusting. The next step is to be SUPER pro-active in researching the different security risks so that you can be aware of what might be going on around you.

Here are popular, most used social media platforms today. What is the most popular activity on these sites? What do you look for when you visit any of these sites. They serve as a primary source of information. We find long-lost friends, classmates, workplace peers, organizations, and family members. We stay in touch with them, sharing our day-to-day routines along with the many accomplishments of our children and grandchildren. We stay in touch with our TSO activities and events through our TSO website. We communicate all types of information to chapter sisters through chapter websites. There are 4.65 billion social media users on the planet. For that reason these sites have developed into top marketing tools for businesses. But it also means that they are top targets for all types of criminal activities. These predators spend their time hacking into these platforms to gain access to us. We have to change our ways and do what is best to protect ourselves, our families, our students, our members.

The new term used today is “sharenting.” The average child has a digital footprint even before they cut their first tooth. For some, it is before they are born. Ultrasound photos announce a pregnancy and gender reveal videos are more popular than ever. Sometimes called a digital shadow or an electronic footprint, a digital footprint is the information about a particular person that exists on the internet because of their online activity. It includes websites you visit, emails you send, and information you submit online. It can be used to track a person’s online activities and devices. Digital footprints are created either actively or passively.

With the advent of social media, two things have changed. First, social media is all-pervasive. You can’t ignore it or put it to one side. Secondly, it can be incredibly difficult to delete content once it’s been posted online. People that like and share your posts are sending your pictures all over the world, to people that you don’t even know. Once those pictures are on someone else’s hard drive, you’ll never be

able to remove it. One activity of cybercriminals is to use information posted to steal children's identities, even when they are grown and independent.

With the increased concern over safety, it's important to remember a few things about children's photos.

- If you take pictures of other people's children, never share them without the parents' consent. For instance, if you take pictures at a sports event or at a birthday party, ask the parents if they are okay with you sharing.
- The same goes for the reverse situation. If you are not comfortable with other parents posting event photos of your children, don't hesitate to ask them to remove them.
- Schools, sports clubs, and other organizations should have their own social media policies in place concerning photographs. As in TSO, there is a statement included on your registration form that you understand your picture may be posted online or in print. Our TSO and ASTEF websites have strict policies that we do not post children's photos, even with parental consent.
- If you have professional photos made of your children, make sure you know their rules about copyright and ask if it's okay to share privately. Some photographers use safe platforms where your family and friends can log in to see photo galleries that are password protected.

With the risks we face today, many parents wonder if they should post pictures of their children at all. Some do choose not to use social media. But if you want to share, there are some tips to help improve the security of your social media.

- Check your social media privacy settings. Restrict your posts to "friends only" and make sure that they don't have the right to re-share your photos.
- Talk to your close friends and family about privacy so that understand your thoughts and wishes on sharing your photos.

- Check your Friends list and remove those people that are not close friends. People you met on vacation who were nice, people who are friends of friends, people you added just to be polite are a security risk.
- Turn off metadata (also known as EXIF, or Exchangeable Image File Format, data) and geotagging for your photos. By doing so, you remove the ability for anyone locating your children using the photo metadata. Or at least ensure that the platform you are sharing from will strip the EXIF data from your photos. Learn all about EXIF data through this QR code.
- Don't include other data that outsiders could use to identify your children, such as their full names, date of birth, or even the school they attend. Use nicknames or descriptive phrases such as "my sunshine" or "our sweet petunia".
- Of course, no nude, or semi-nude photos should be posted of your children. Those "baby in the bathtub" pictures are cute for grandparents, but very risky for the rest of the world.

When you are taking photos, pay attention to any identifying items in the background of the photo, such as street names, building names, store signs, etc. School uniforms are another way of identifying locations. When looking at the list from the first slide of popular social media platforms, this is a good time to point out that WhatsApp allows you to give selected friends access to your photos, and the service is encrypted end-to-end to avoid hackers accessing your data. Have you seen their commercial lately? There are also private, invitation-only online albums such as Flickr. Another popular photo-sharing app is Tinybeans. It allows you to set up a private group and create something very similar to the baby books used in the past. It was started in 2012 and now has over 3 million users who take advantage of its invitation-only base and its security.

We also need to consider the risks of hackers gathering personal information. The first step is to be aware of what types of threats are being used so that you can be prepared to recognize them when you become the target.

- Social Engineering
    - The attacker fools the victim through impersonation. They may pretend to be your boss, your supplier, or your delivery company.
- Phishing
    - This is the email or text message you receive trying to entice you to click on a malicious link or open a malicious attachment. The attacker also applies pressure by creating a sense of urgency or appealing to their curiosity.
    - “Act now before it’s too late” “Your friend died in an accident”
- Malware
    - Malware is malicious software that can be downloaded to your computer when you click on a link downloading viruses, trojans, spyware and ransomware.
    - Cyber criminals use malware to access your devices and networks to steal data and take control of systems or damage systems.
- Brand Impersonation
    - An individual or group tries to impersonate a well-respected company or brand to trick victims into providing confidential and valuable information that can be used by social engineers to hack systems and networks.
    - Not only does this type of attack harm the victims, but it also damages the reputation of the organization being impersonated.
- Catfishing

- The cybercriminal takes information and images from another to create a fake identity and then uses it to victimize an individual on a social media platform.

As I said, being aware of the different types of threats and how they work is the first step in protecting yourself from these cyber threats. But there are more steps that you can take to address these threats.

1. Enable MFA. Multi-factor authentication requires users to provide two or more authentication factors to access an application, account, or virtual private network. This step adds extra layers of security to prevent more sophisticated cyberattacks even if your credentials or identities have been stolen, exposed, or sold by third parties.
2. Do not re-use passwords. Use a different password for every account. By using one password for all accounts, you are opening opportunities for hackers to access more accounts. Use a notebook or an online password manager to keep up with your passwords. PC Magazine rates these password managers as the best for 2023. Be sure to check each one because they are used for different situations.
    a. Bitwarden – best for free password management
    b. Dashlane – best for security-focused extras
    c. Zoho Vault – best for sharing features
    d. 1Password – best for password organization
    e. Keeper Password Manager & Digital Vault – best for secure cross-platform password management
    f. LogMeOnce Password Management Suite Ultimate – best for abundant features
    g. NordPass – best for business account administrators
    h. Password Boss – best for browser tools
    i. RoboForm Everywhere – best for form-filling capabilities

3. Regularly update the security settings. Stay on top of social media platform security options to make sure your settings are always current and set at the strongest level.
4. Narrow down connections to reduce unknown threats. Be wary of the types of individuals and entities that you are connecting with on your social media platforms. Always review every connection, and don't affiliate with those that seem to be disingenuous or suspicious.
5. Monitor social media for security risks. As I said before, research. Make sure you know what security risks are most relevant to your platforms. As you hear of threats happening, check your accounts and address any issues that might lead to breaches or hacks.

6. Learn what a phishing attack looks like. Be diligent and learn the latest types of phishing attacks going on. Always be skeptical when someone reaches out to you uninvited through a social platform, text, or email.
7. Look out for spoofs of your account. Keep an eye open for brand impersonation attempts. Go ahead and report violations to the social media platform administrators immediately. Inform your followers as well.

That takes care of some of the more personal issues concerning web security, but what about your business, your chapter, your church, your school? Since the pandemic, social media has been utilized for all people to stay connected through the internet. Again, we have the increase in use resulting in the increase in risks. As organizations, whether business or social, it's important to build social media strategies to protect accounts from hacking, phishing, and malware. As I said at the beginning, it's also important to remove risks for your members. The same policies that apply to children can apply to adults. The chapter president I mentioned was notifying her members of the location, date, and time of their chapter meeting. It took no time at all for someone to notice that information and contact her directly through messenger.

I want to emphasize more on why the digital footprint matters. They matter because:

- They are relatively permanent, and once the data is public—or even semi-public, as may be the case with Facebook posts—the owner has little control over how others will use it.
- A digital footprint can determine a person's digital reputation, which is now considered as important as their offline reputation.
- Employes can check their potential employees' digital footprints, particularly their social media, before making hiring decision. Colleges and universities can check their prospective students' digital footprints before accepting them too.
- Words and photos which you post online can be misinterpreted or altered, causing unintentional offense.
- Content intended for a private group can spread to a broader circle, potentially damaging relations and friendships.
- Cybercriminals can exploit your digital footprint—using it for purposes such as phishing for account access or creating false identities based on your data.

This is exactly why you must consider what your digital footprint says about you. One of the best ways to manage your digital footprint is by being cautious about your online activities to control the data that can be gathered in the first place.

Your internet activity can involve hundreds of items that will form part of your digital footprint. Think about where you go on the internet: online shopping, online banking, social media, reading the news, health and fitness just to name a few.

USED:

https://www.fortinet.com/blog/industry-trends/7-best-practices-for-social-media-security-and-privacy#:~:text=Use%20a%20different%20password%20for,update%20security%20settings%20across%20platforms.

https://www.pcmag.com/picks/the-best-password-managers

https://www.searchenginejournal.com/social-media/biggest-social-media-sites/#close

https://usa.kaspersky.com/resource-center/threats/children-photos-and-online-safety

https://consumer.ftc.gov/consumer-alerts/2022/10/five-things-do-protect-yourself-online

https://blog.hootsuite.com/social-media-security-for-business/

https://www.cnbc.com/2016/08/15/why-you-should-think-twice-before-posting-that-picture-on-social-media.html