Social Media Dangers: WHAT EVERY SOCIAL BUTTERFLY SHOULD KNOW

Social Networking Security Risks—Best Practices for Creating a Culture of Security

2019

DIGITAL DEFENSE INCORPORATED

DigitalDefense.com

888-273-1412

Friending, following, tweeting, instagram-ing, checking-in and linking up....In today's ever connected world, people all over the globe are utilizing social media.

Many businesses today leverage social media for various marketing purposes. As social media platforms have expanded to focus on particular niches such as photography, videos or even business networking, adoption and user stickiness have increased and additional risks have followed. Social media users are not only your customers but also your employees.

Social media, although still growing and evolving, is here to stay. The goal of many organizations is finding a balance between encouraging employees to utilize social media for business, while staying mindful of the potential security issues. Hackers know that an employee is truly the first line of defense for any company and therefore a vulnerability they can exploit, and consequently target those employees who may not be as careful as their co-workers with what they share.

Employees can be quick to bring social media usage into the work place, creating a hot-spot of potential security vulnerabilities and new attack vectors.

There are various ways to fool employee social media butterflies into putting a company at risk, but there are also ways to head these threats off at the pass. Knowledge is power!

The best way to avoid unwanted attacks is to understand the dangers of social media, with a security lens applied, and implement solutions and best practices for smarter socializing. Because all businesses are made of employees (from head to toe), this eBook will address best practices for safer social media engagement.

In this eBook, we look at the following:

- Today's primary tactics used to exploit online social networks.
- Real World Scenarios of Social Engineering via Social Media sites like Facebook, Twitter and LinkedIn.
- Best practices to mitigate risks social media platforms can create.

SOCIAL BUTTERFLIES BEWARE

Everyone's a social butterfly to some extent these days, some more than others. There are many benefits to using social media platforms, but there is also a darker side.

The reason social media platforms are so successful is because they tap into the human sense of needing to feel accepted by others. Consequently, you can count on your employees accessing one or more platforms throughout the workday.

Just as this need is ingrained into our psyche, social media is now ingrained into our everyday lives. New social platforms often seem to spring up overnight and gain adoption quickly, and the social media footprint for people is only increasing.

Whaling and clickjacking.....No, these are not episodes of a reality show on a sports and outdoor channel. These are uncommon names for common tactics used by social hackers leveraging social media channels to gain access to sensitive data with more nefarious interests than simply liking a post or commenting on a photo.

These social engineering gurus are utilizing social media sites such as Facebook, Twitter, Instagram, LinkedIn, etc. to track and attempt to take down entire organizations, and it all starts with one trusting person.

TRICKY TRICKS OF THE TRADE

Sharing is caring...right? Not always.

Social Engineers (AKA: Hackers) do not care if you are an entry-level employee or the CEO of an enterprise because chances are you are connected to someone with power or something of value. These highly trained individuals leverage their skills to attack all levels within an organization through new media and online tactics. Using proven methods, they can gain access to sensitive information, destroy reputations, and cost enterprises billions in cleanup and recovery.

Phishing

Though this tactic isn't new, it's expanded from email into social media platforms. It occurs when a user receives a fake message from a hacker or social engineer posing as a colleague. The message may contain a nefarious link leading you to an unsecure page containing vulnerabilities.

Clickjacking

The concealment of hyperlinks beneath legitimate content that leads the user to unknowingly perform damageable actions such as downloading malware or sending your ID to a site. Numerous clickjacking scams have employed "Like" and "Share" buttons on social networking sites.

Elicitation

Back-in-the-day we called this “chatting”. Today, this is a strategic use of written conversation to extract information from people without giving them the feeling they are being interrogated. This could happen via any social media platform that has a private messaging (PM) feature.

Profile Hacking Scams

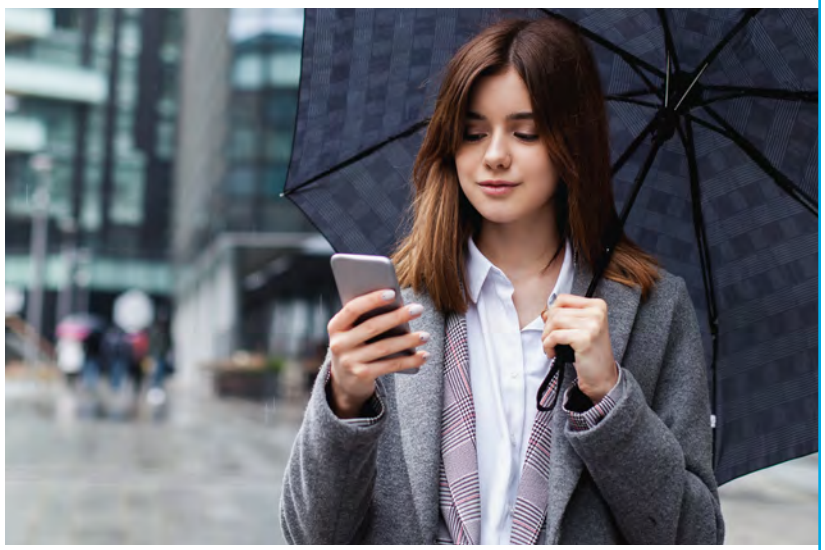
Facebook, LinkedIn and many other social media platforms rely on profiles. Cyber-criminals use real photos and characteristics of very real people to create a profile and entice users to connect with them, all the while planning to steal from the individual or someone in the individual’s network.

This type of scam usually tricks people into giving them money with a wire transfer or even another social application such as a GoFundMe campaign. If your employees are connected to your network when using social media, especially with their personal device, this opens up yet another vulnerability to your organization, especially if financial transactions are taking place.

ATTENTION EMPLOYEE - DOES THIS SOUND LIKE YOU?

You arrive at the office. It is cold and rainy outside. Once again the security guard who unlocks the door to the office building is late. You are bored and frustrated so you pull out your smart phone and Tweet to the world,

"Grrrrrr. 😡 I hate waiting for the security guard who is always late! #atmyoffice"



Your friends may laugh, sympathize or even comment. Seems harmless, right? After all, sharing your life isn't a bad thing because you trust your social contacts, and they share their life with you online too. But it can be very dangerous.

You may have unwittingly exposed your employer and yourself to a security attack. But it is random, rare, only something you read about. Think again. Information is power and, in this scenario, you just provided a potential hacker with key insight into not only your schedule but also your employer's potential vulnerabilities and a possible attack vector due to the lack of vigilance and your "over sharing".

This all can be used as inside knowledge when searching for vulnerabilities and planning an attack.

"Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you become." – FBI

ATTENTION EMPLOYER - DOES THIS SOUND LIKE YOU?

Your business is growing. You are looking to hire new employees to help you meet market demands. Like most in your industry, you post a job description for the new employment opportunities on your corporate LinkedIn page.

You receive a candidate response via email. You open that email. That email has malware connected to a Trojan which, according to the FBI, is commonly used by cyber criminals to defraud US businesses. The CFO opens the embedded malware, which allows the social engineer to obtain online banking credentials, consequently costing you thousands of dollars.

"Malicious attachments have become such a problem that many organizations now require job seekers to fill out an online application rather than accept resumes and cover letters in attachments."

– Chris Hadnagy author of Social Engineering: The Art of Human Hacking

COMMON SOCIAL MEDIA SCAMS IN 2018

Fake News

Propaganda is not new, but the platform used to spread it is. Fake News can spread like wildfire via social media channels because the titles are usually so outrageous people find it hard to not read it and then not share it. If an employee shares fake news within your organization, it can cause damage to your brand.

"In a virtual environment where several human senses are ineffective, the ability to verify the entity on the other end of a conversation is compromised...The fake news problem is no longer a sociopolitical issue, as it is now a component of much larger cybersecurity problems that have been left unchecked for too long." – TechTarget

Quizzes That Mine Your Information

According to Security Intelligence and IBM, this scam is focused on creating and pushing out popular quizzes on social media that have been widely shared on various social media channels. They are imploring users to take a few minutes for what seems like harmless fun.

"The Better Business Bureau (BBB) warns that some quizzes are designed to steal your data in an outright scam. Oftentimes, cybercriminals will include links embedded in the quiz that can steal information from your personal accounts. Once these criminals have your account information, they can use it to lure in other unsuspecting victims, including your friends."

– SecurityIntelligence.com

URL-Shortening Cons

Marketing teams often use URL shorteners, and though very helpful in sharing a long website link within a tight character limit on social media platforms such as Twitter, they can also mask a malicious webpage because you never know where the site could actually lead. According to Security Intelligence brought to you by IBM, "That location could be a nefarious site run by cybercriminals that can drop malware on your machine or lead you into some other scam. If you're concerned about a shortened link, you can check it before clicking. There are a variety of websites, such as CheckShortURL, that offer a URL lengthening service, enabling you to paste in a link to see exactly where it leads."

SAFER SOCIALIZING

Be Mindful of Your Check-Ins

Many utilize social media sites that allow users to “check in” at restaurants, retailers and event locations. Some engage for discount incentives, while others do it to let their friends and family know their whereabouts. What most people fail to remember is that this information is intelligence for those looking to better understand your schedule, habits, and potential opportunities for strategic cyber-attacks.

In recent history, criminals are leveraging social media location statuses to orchestrate strategic physical security attacks on homes, hotel rooms, etc. We’ve even seen some celebrities fall victim to physical robbery recently, due to this kind of attack.

Activate Privacy Settings

Look at the privacy settings for the social media services that you utilize and make certain that you are only sharing information with people you know. Also, check to see your privacy settings on each social media platform that is connected to another social media platform. How are they sharing your data with one another?

Blind Trust is Extinct

Verify with the users before you open attachments sent to you via social media channels. Make sure the person you think sent it to you really did by reaching out to them via a non-social media channel. Ensure you do not blindly click or share news that might sound sensational. Search the internet for another trusted source first.

Password Protection

Don't forget about the importance of utilizing a secure password for your different social media accounts. If your password is your first born son's name or the college you attended, this is like giving candy to a baby when it comes to the mind of a criminal hacking into your account. Focus on a phrase that has a mix of letters, numbers and special characters. For example, if you like The Wizard of Oz, create a password like this: W1z@4d0f0z!.

Ethical Hackers

Businesses should consider contracting with ethical hackers or white hat hackers to employ social engineering techniques to identify vulnerabilities so they can address them before hackers are able to exploit them.

Security Awareness Training

Organizations should consider creating security awareness training for their employees to educate them on best practices for social media, though it should not stop there. If employees are not educated, it is easy for them to think something from a hacker is harmless and, by acting on it, put the business at serious risk.

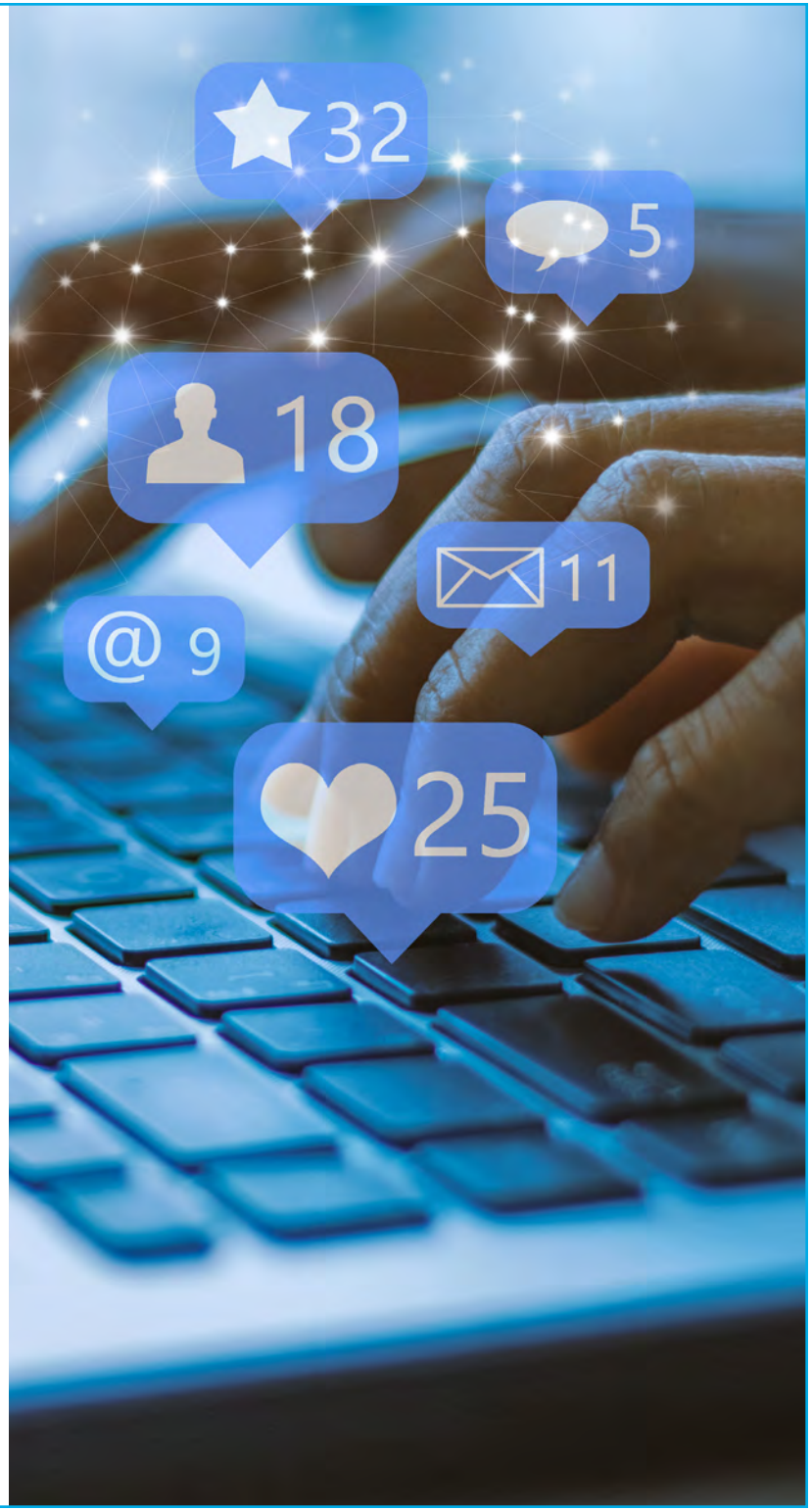
SOCIAL MEDIA TO-DOS AND TO-DON'TS TO SHARE WITH YOUR ORGANIZATION

- Leaders, establish clear policies about what company information can be shared on blogs and personal social sites. Stay diligent and enforce them.
- Do not share personal information about yourself, family and friends, be it online, in print or in person.
- Type the URL into your browser to view vs. clicking on a link shared via social media or email.
- Get to know your co-workers and clients, and beware of digital impersonators. Do they pass the sniff test? Trust your gut and validate.
- Disable Global Position System (GPS) coding in items that you might not normally think of such as your cell phone camera.
- Provide or take annual security awareness training.
- Avoid accessing banking accounts from public computers or through public Wi-Fi spots.
- Don't provide information about yourself that will allow others to answer your security questions (I forgot my password key questions).
- Report suspicious incidents to your security team.

WRAPPING IT UP

In closing, social media is for sure not going anywhere—if anything it is just getting deeper and wider. That said, there are many recent compliance mandates and laws that have been put in place to create guidelines for how data is shared and used in social media, as well as all sites that contain sensitive information. But it traditionally takes companies time to implement these controls, and they certainly don't protect you from everything. Attackers get smarter by the day, and the social media threats have only evolved since they've become mainstream.

Social media is a great way to stay in touch with your family and friends and share your life. It's also a great way for businesses to reach new customers and efficiently zone in on their target audience. Businesses and individuals can continue to leverage social media, but both should just make sure they are sharing things with the right people by following these best practices.



KNOWLEDGE IS POWER

Social media is here to stay, be it at home or at the office. Social Engineering, system compromises, employee and third-party negligence are all contributing factors to security breaches. Just as it is important for organizations to protect their networks from attack, it is essential that they effectively educate their employees to fend off costly attacks that target employee vulnerabilities.

Effective security awareness training for your employees and clients can improve your overall security posture, and it could be the most important investment you make this year.

Digital Defense's Security Awareness Training Program, SecurED® helps organizations provide relevant, entertaining, web-based training that helps to establish a culture of security.

SecurED

Resources and References

http://www.ijirst.org/articles/SALLTNCSP031.pdf

http://www.harbus.org/2018/beware-social-media/

https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media

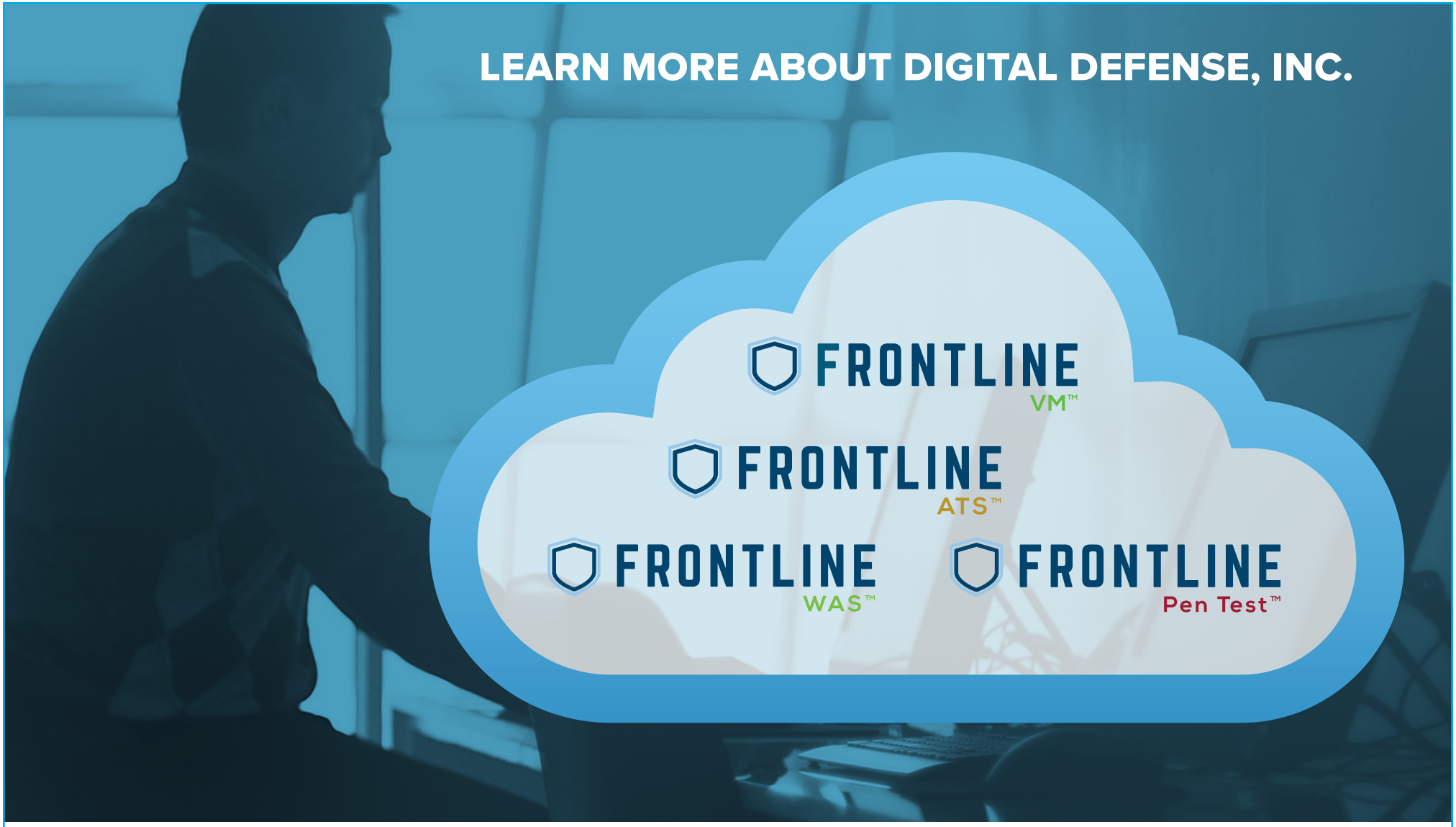
https://searchsecurity.techtarget.com/tip/How-new-cybersecurity-problems-emerge-from-fake-news

https://support.gofundme.com/hc/en-us/articles/115015913668-How-to-Determine-if-a-GoFundMe-is-Safe-to-Donate-To

https://securityintelligence.com/what-are-the-seven-biggest-social-media-scams-of-2018/

https://www.techadvisor.co.uk/how-to/social-networks/how-avoid-common-snapchat-scams-3676895/

https://archives.fbi.gov/archives/news/testimony/the-fbis-efforts-to-combat-cyber-crime-on-social-networking-sites -



www.DigitalDefense.com

DIGITAL DEFENSE® INCORPORATED

9000 Tesoro Drive, Suite 100, San Antonio TX 78217
Toll Free: 888.273.1412