Social Media Security

Information Security Awareness

Course Goals

- This course sets out the rules, guidelines and risks associated with social media. It suggests ways to use these technologies in a productive manner while ensuring the security of your personal and organizational information.
- Just as there is a need for training in email etiquette and email security, engagement in social media requires the application of etiquette and security awareness. We all need to be vigilant in keeping our protections current as well as avoiding risky or embarrassing activities.
- Upon completion of this course, you should be able to engage in social networking confidently and professionally whether for personal use or on behalf of your employer. You'll also understand the associated risks in order to make wise decisions.

Topics

- Section 1 covers:
  - An explanation of social media & the value it brings to businesses
  - The threats, risks & vulnerabilities inherent in the technologies
  - Information regarding compliance, penalties & fines
- Section 2 covers:
  - Social media & cybercrime, threats & malware
- Section 3 covers:
  - How to safely engage in social media without putting yourself, or your organization, at risk

Social Media vs Social Networking

Section 1

What is Social Media?

- Social media is a **tool**
- Social media is a dynamic web-based tool used to facilitate the two-way communication. We also reference it as social networking.
- Businesses use social media to expand their contact base and leverage their brand. Social media tools are quickly replacing traditional promotional tools like TV and magazine advertising, and direct mail.

What is Social Networking?

- Social networking is the **act of engaging in 2-way communication**
- A social networking website is a platform that focuses on building social relationships among people who share common interests and/or activities. Social media “tools” (such as forums) facilitate this interaction.

Characteristics

- **Reach** – capable of reaching a global audience
- **Accessibility** - social media tools are generally available to the public at little or no cost
- **Usability** – requires no specialized skills or training; anyone with Internet access can participate in social media production
- **Immediacy** - capable of offering virtually instantaneous web-based communication
- **Permanence** – posts can be altered almost instantaneously by comments or editing; users must use caution, because what you post online will stay online – forever.

Social Media Growth

- Active social media users have passed 4.55 billion users
- People spend an average of 2 hours and 27 minutes on social media a day
- 98.3% of Facebook users use their mobile phones to view the social platform
- 100 million users launch or watch live videos on Instagram everyday
- Twitter has 211 million active users a day
- LinkedIn owns more than 800 million active users in 200 countries and regions worldwide

Businesses & Social Media

- Company's now use social media to:
  - Improve communications to its existing client
  - Expand their reach to new customers
  - Run campaign ads
  - Post updates, new features and upcoming events
  - Run clientele report data reports
  - Accept donations and payments
- & much more

Social Media Threats

- People share more personal information on the internet than ever before
- People trust social media sites too easily with personal and confidential information
- Lack of social media policies – organizations don't outline or secure their policies enough
- Mobile Apps – there is no guarantee that downloaded apps don't have bugs or malware installed already

Privacy

- Employers are increasingly taking proactive measures to ensure security and regulatory compliance which obligates them to monitor, manage and archive what's being communicated to, from and within the enterprise.
- As a result, employees have no reasonable expectation of privacy when they're using corporate systems and networks.
- Therefore, you can expect that what you post on social networking sites while using corporate assets is being monitored and archived in accordance with regulatory mandates.

Beware of Social Engineering

- Social engineering is a collection of tactics used by hackers to manipulate people into performing actions or divulging information that is then used to gain access to a computer system or a facility. In most cases, the attacker never comes face-to-face with the victim who seldom realizes they have been manipulated.
- A hacker may have to invest a lot of time and effort in breaking an access control system, but he or she will find it much easier to persuade a person to allow admittance to a secure area or to disclose confidential information.
- Hackers exploit human behavior using social engineering tactics to breach an organizations' security defenses.

Beware of Suspicious Links & Ads

- When in doubt, never click on a suspicious link even if it comes from someone you know. Suspicious links can contain a masked link to an infected or phony website that mimics a real site. Malicious webmasters can also use HTML, Flash or Java Script to mask or change a browser address.
- You may be able to tell if a link is real by moving your mouse over it and looking at the bottom of your browser to see the hidden Web address - it will look different than the one you see on the surface.

Your Part in Ensuring Security

- Technology alone cannot protect your personal or work information from being exploited; a great degree of responsibility lies in the hands of the user.
- Both individuals and organizations are at risk because securing your personal and work resources is as much a human issue as it is a technology issue.
- Inappropriate use, errors in judgment and inadequate security controls can mean non-compliance with government and industry regulations resulting in hefty fines for organizations, potential loss of business and fraud.
- Individuals are also at risk of ID theft, home burglary, viruses, malware and personal monetary loss.

Your Part in Ensuring Security

- Other risks include:
  - Copy-right and trademark infringements
  - ID theft
  - Loss of intellectual property
  - Violations of industry-specific regulatory requirements
  - eDiscovery costs
  - Reputational risks
  - Data breaches
- & more

Your Part in Ensuring Security

- Businesses must work harder to transform employees into data security ambassadors by giving them a clear set of guidelines on how to engage in social media safely and smartly both at home and at the office.
- Companies are more closely managing the use of these technologies, making sure to follow industry and regulatory best practices for logging content, blocking threats, preventing data leaks, archiving content and controlling their use.

Compliance

- **GLBA** requires financial institutions to develop a written information security plan that describes their plans to protect clients' private personal information. SEC & GLBA adopted Regulation S-P to protect non-public consumer information.
- **SOX, SEC and FINRA Rules** - obligating organizations to preserve all records (workpapers, memoranda, correspondence, electronic records) for a minimum of six years. Correspondence with the public must be supervised, reviewed and retained.
- Preservation of email communications and IM conversations for more than 10 years. SEC & FINRA are extending these rules to social networking. This means that email, IM conversations, posts to SM sites and other content must be retained and managed in such a way that it is easily-accessible and can be produced on demand.
- **PCI DSS** – protects payment account information and includes provisions for encrypting cardholder data.
- **Red Flag Rules** – require financial institutions to detect, prevent and mitigate instances of ID theft which includes protecting instant messaging and social media tools from malware that could allow criminals access to confidential information.

Compliance

- Not obtaining compliance can lead you and your organization to:
  - Substantial fines
  - Imprisonment
  - Loss of reputation
- & more

Your Part in Ensuring Compliance

- Compliance is "doing the right things, the right way”
- Employees are now, more than ever, under tremendous pressure to ensure their behavior on social media sites are in compliance with organizational policies and federal, state and industry regulations.
- Each employee has the responsibility to uphold their organizations’ policies and core values of integrity when participating in social networking activities.

Cybercrime, Threats & Malware

Section 2

The Origins of Malware

- **Email Attachments** – before opening, ensure that attachments you receive are legitimate
- **Portable Media** – any device that can store information can support malicious content
- **Visiting Malicious Websites** – any legitimate website can be the victim of an attack, which in turn could leave you at risk
- **Downloading Files from Websites** – including generic files, software, plug-ins, movies, audio files, as well as mobile code such as ActiveX, JavaScript, Flash etc
- **Participating in P2P File Sharing Services** – peer-to-peer file sharing systems, especially when used to access illegal or infringing content

The Origins of Malware

- **Instant Messaging Clients** – especially if unpatched, they allow hackers to upload or download files through holes in the client software.
- **New Devices and Peripherals –** although it's rare, mobile phones, digital photo frames, etc can be compromised during manufacturing if the manufacturer's system is infected.
- **Social Networking Sites** – offer several situations that could put you at risk of infection
- **Social Engineering Attacks –** that trick users into either giving up information or unwittingly performing tasks that result in a security breach
- **Not Following Security Guidelines and Policies** – bypassing filters, using unauthorized outside storage devices, blocking software updates, using non-approve software clients, etc, increase the chance of becoming infected by malicious code

Be Aware

- Don’t click on random websites you see shared on the internet; people could be sharing infected links
- Don’t click or take surveys from noncredible sources
- Don’t sign up for any “FREE” giveaways
- If you can’t verify it veracity don’t click on it

The Faces of Cybercrime

- The virtual criminal community is highly organized, with millions of dollars being generated by tightly coordinated groups of specialists, all syphoned by naive money mules into bank accounts around the world.
- The cybercrime phenomenon will continue to grow, with virtually no barrier to entry, potentially limitless spoils, and a slim risk of getting caught.
- Cybercrime is expanding rapidly across a wide spectrum including online fraud, intellectual property rights (IPR) matters, computer intrusions (hacking), economic espionage (theft of trade secrets), confiscating online bank accounts, child pornography, international money laundering, identity theft, and a growing list of additional criminal and civil matters.

The Faces of Cybercrime

- As important as it is to understand the prevalence and monetary impact of cybercrime, it is also vital to gain insight into who the typical perpetrators are. The common adage, “know your adversary,” is as true for cybercrime as it is for warfare.
- Hackers are motivated to do what they do for different reasons, such as money, ego, revenge and curiosity. The professional cybercriminal, however, is motivated by financial gain.
- Because cybercriminals continue to refine and fine-tune each element of the cybercrime supply chain, users must be educated and alert

The Faces of Cybercrime

- The massive amount of personal information online coupled with the lack of user knowledge of how to secure this data will continue to make it easy for cybercriminals to engage in ID theft and user profiling.
- Targeted phishing attacks are moving to technologies like Facebook and Twitter because choosing users and groups to exploit through these channels is simple.
- Targeted attacks on major corporate bodies are developed in military-style operations using intelligence that has been gathered using publicly-available information on social media sites

The Cost of Cybercrime

- Cybercrimes can do serious harm to an organization's bottom line.
- A recent Varonis study shows cybercrime hit $6 TRILLION in 2021.
- Anyone who uses the Internet is susceptible to Internet crimes. Likewise, anyone who uses social media is susceptible to social networking crimes.
- A Cybint study shows that 95% of cybersecurity breaches were caused by human error. A great deal of time, effort and money can be saved by ensuring that everyone is aware of the threats and what they can do personally to minimize the risks.
- Next, we'll look at how you can help minimize the risk when engaging in social media networking.

Engaging in Social Networking

Section 3

Setting Up Your Profile

- The following best practices apply to all social media sites, including but not limited to Facebook, Twitter and LinkedIn:
- Choose a strong password: Make it longer than eight characters, include a variety of letters, numbers, and symbols, and change it regularly. Make sure you use different passwords for your different online accounts.
- Never save passwords in your browser: Browsers often ask if you'd like to save your password for easy access (so you don't have to enter it on your next visit). Never ever save your passwords on your computer.
- Never post information in your profile (or elsewhere) that could be used to confirm your identity. This includes home address, birth date, phone number, etc. An individual's DOB and state of birth are enough to guess a SSN with great accuracy.
- Turn off the bells & whistles. Disable options, then open them one by one.
- Set up login alerts. To help protect your account, request an email from the site should someone try to login from an IP address other than yours.

Editing Your Privacy Settings

- Use your privacy settings to control who gets to see your posts and profile.
- Turn off applications such as games & quizzes (Get a free goat on Farmville!). If you choose to add applications, ensure you understand and control how much information you share with the application.
- Enable secure browsing, or HTTPS when using social media sites from unsecured public networks such as those in airports, cafes or hotels. This encrypts the information you send and receive. (Look in the site's security settings)
- Get tips and advice on how to avoid threats from the site's security/privacy page.

Friends & Contacts

- Use discernment when accepting friend invitations. Only accept invitations from people you know. Cybercriminals create bogus profiles to propagate malware.
- Show “limited friends” a cut down version of your profile. This can be useful if you have associates to whom you do not wish to give full friend status.
- Remove a connection to a friend that you are no longer comfortable with.
- Block individuals if they are harassing you or if you just don’t want to be visible to them.
- Report abuse: The most efficient way to do this is right where it occurs – in the social media site’s privacy settings.

Proceed with Caution

- Be careful where you click. Make sure to evaluate the potential costs/benefits of pop-ups, applications, and invites.
- Don’t be an early adopter of a new app. Give the community time to discover the security weaknesses before you dive in.
- Avoid suspicious-looking URLs. Make it a habit to mouse over links to identify the source and proceed with caution.
- Never click on unsolicited links containing celebrity gossip, natural disasters, political scandals etc. Scammers quickly build malicious websites designed to trick users into installing malware or sending donations to replicated websites.

Proceed with Caution

- Never copy & paste a link into your address bar unless you know where the link goes. Doing so will bypass your browser's security controls.
- Never post your whereabouts or your vacation plans. You're only helping burglars to plan their break-in.
- Never give up your login credentials. Social engineers are equipped with enough information to trick you into believing the request is from a legitimate authority.
- Ask permission before posting someone's picture or publishing a conversation that was meant to be private.
- Respect the law, including those laws governing defamation, discrimination, harassment and copyright.

What NOT To Say

- It’s easy to say or do the wrong thing. An online mistake can show up next to your name in an Internet search for years to come. Protect yourself & others by following these guidelines:
- Practice prudent posting. Use your best judgment – remember that there are always consequences to what you publish.
- Use common sense. Don’t use ethnic slurs, personal insults obscenity or engage in questionable behavior.
- Show respect for people’s privacy and for topics that may be considered objectionable or inflammatory, like politics and religion.
- Don’t pick fights. Be the first to correct your own mistakes and don’t alter previous posts without indicating that you have done so.
- Don’t post about your coworkers, especially negative comments, as this might create a hostile work environment. Also, a bad or poorly-stated remark could compromise the whole organization.

Posting on Behalf of Your Employer

- If your job function allows you to post on behalf of your employer, follow these guidelines:
- Identify yourself as an employee & state your position in the company. Do not use pseudonyms or false screen names.
- Ensure your profile and related content is consistent with how you wish to present yourself with colleagues and customers.
- Don’t reference staff, partners, vendors or customers without their approval.
- Never reveal information that compromises your organization’s policy or public positions, meaning anything that is proprietary and/or confidential.
- Respect the diversity of opinions. Conduct yourself & your conversation in a professional manner at all times.
- Never conduct confidential business with a customer or business partner through a social media site.
- Ensure that your conduct is consistent with the policies contained in your employer’s Employee Handbook.

Final Points

- It is important to remember that while social media security (and web protection in general) is an important element of IT security, it is only one facet of IT security and business risk management as a whole.
- While an organization may not have been subject to attack, there is no room for complacency. This is not about panic but being sensible – we can equate IT security with driving a car appropriately fitted with seat belts and air bags. We hope you will never need them, but we all feel more comfortable when they are in place.
- Hopefully, the information and advice included here has helped you to better understand the issues that exist, and to adopt appropriate online behavior to mitigate the risk.

CONGRATULATIONS

This concludes the course on “Social Media Security”