RIVER BANK
We Bring Banking to You!

SAFELY USING SOCIAL MEDIA

People are revealing too much information online. Users of social networking sites may not think much about the way posted information might enable identity theft, home burglary and social engineering attacks and may easily get into trouble. Neither do they consider how their behavior on social media sites might affect their employer. Information security awareness training can help to decrease the likelihood of serious problems whether at home or at work.

Social technologies introduce a number of threats. Here are the top five:

1. **Mobile Apps -** There's no guarantee that mobile apps are free of bugs or malware. Mobile malware is capable of obtaining any and all permissions on the infected device, sending SMS messages to premium phone numbers, stealing online banking credentials & downloading other malicious code without the user's knowledge.
2. **Social Engineering -** Social media has taken this threat to a new level for two reasons: 1) People are more willing than ever to share personal information about themselves online, and 2) social media platforms encourage a dangerous level of assumed trust.
3. **Social Networking Sites -** Sometimes hackers go right to the source, injecting malicious code into a social networking site, including inside advertisements, shortened URLs, and via third-party apps.
4. **Users –** It's imperative that users understand how to safely navigate the Internet. At the same time, individuals & employees need to behave responsibly, understanding that we all have lapses in judgment, make mistakes or behave emotionally. Nobody's perfect all of the time.
5. **Lack of a Social Media Policy –** Organizations need to spell out the goals and parameters of their enterprise's social media initiatives or they're inviting problems. Employees need proper training, if only to clear up issues regarding official social media policies, and every social media initiative needs a coordinator, i.e. a social media manager.

Undoubtedly, the use of social networking increases the risk of leaking sensitive information and PII. There are other risks to organizations as well:

- Reputational risks
- Data breaches
- ID theft

- Copy-right and trademark infringements
- Defamation and libel
- Loss of intellectual property
- Violations of industry-specific regulatory requirements
- eDiscovery costs.

Apply the following best practices to all your social networking accounts and activities.

1. Setting up your social networking account:

- **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 each of your 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.
- **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.

RIVER BANK
We Bring Banking to You!

2. **How to safely engage in social networking:**
    - **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.
    - **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.
    - **Never copy & paste a link** into your address bar unless you know where the link goes. Doing so will bypass you 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.

RiverBank has taken strong measures to ensure the security and safety of your account and its overall online banking system. Follow good practices and use the knowledge we've provided here, and you will be much more prepared to enjoy the conveniences of online services with peace of mind!