Social Media Security Tips

All of us serving you®

usbank®

Don't Let Social Media **Put you at Risk**

People use social networking sites like Facebook and Twitter to connect with others and share photos and personal messages. As these sites increase in popularity, so do the risks of using them. Follow these security tips to help protect yourself when you use social media.

1. Use strong passwords

- A strong password is a combination of letters, numbers, and symbols.
- Avoid using phrases that can be easily guessed.
- Use a different password for each service, and change passwords periodically.

2. Select secret answers

If a site requires a security question in addition to a username and password, pick the most obscure question, or type your own question if allowed. Never select a question with information found in public records or online, such as your mother's maiden name. If necessary, make up an answer or use letters, numbers, and symbols.

3. Keep software up-to-date

Install software updates on all your devices, such as your smart phone, PC, and laptop. (This is especially important for web browsers.) If your operating system offers automatic updates, enable them. Maintain anti-virus software to protect against new viruses.

4. Be wary of add-ons

Social networking sites often allow you to download third-party applications to enhance your personal page (for example, send greeting cards). Research any file before you download. Rogue apps can access your contacts to send spam messages or steal data.

5. Never share confidential information

Never reveal private information such as your passwords or your Social Security number. Don't post personal details. Thieves "data mine" information from different sites to learn your habits and trick you into divulging confidential information.

6. Customize settings

A site's default settings may allow anyone to see your profile. Set security options to limit access to your profile. These sites collect your information and may share email addresses or user preferences with other companies. Review the site's privacy policy and adjust the privacy settings. Review your settings periodically to keep up with changes in how your information is protected.

7. Treat posts as public and permanent

Anything you post online – including blogs, tweets, or photos – may be widely disseminated. Don't reveal information that could endanger you, like your location or schedule. Even if you delete your account, others may have saved your particulars. Remember, once something is on the Internet, it can never be fully removed as others may have re-posted, re-tweeted, or copied the information or object.

8. Choose friends wisely

Some cyber criminals use friend requests as a way to get inside social networks so they can disseminate malware or steal information. If you befriend strangers, create a lower-level contacts group and share only limited information.

9. Be leery of all links

Treat links to videos, games, or other files you receive in social media messages – even from friends – as you would suspicious links in email messages. Check with the sender or search online to find the file yourself.