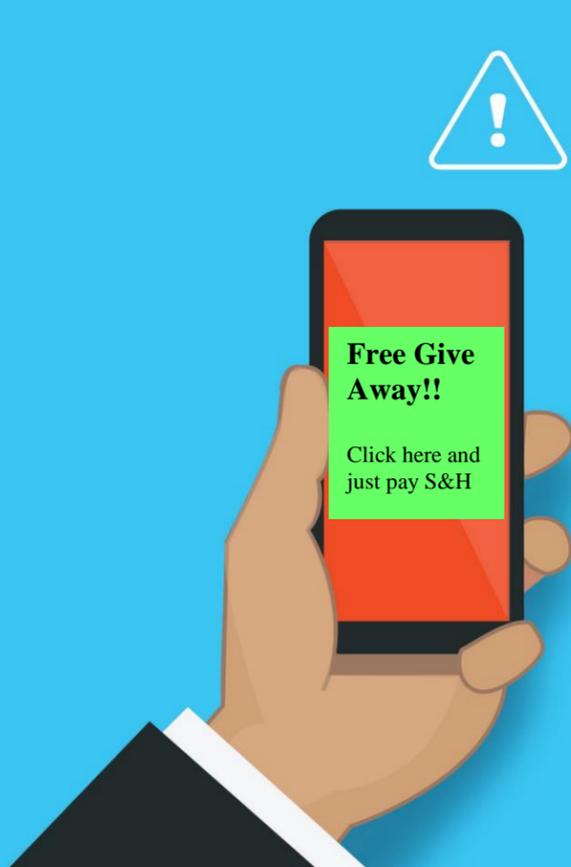
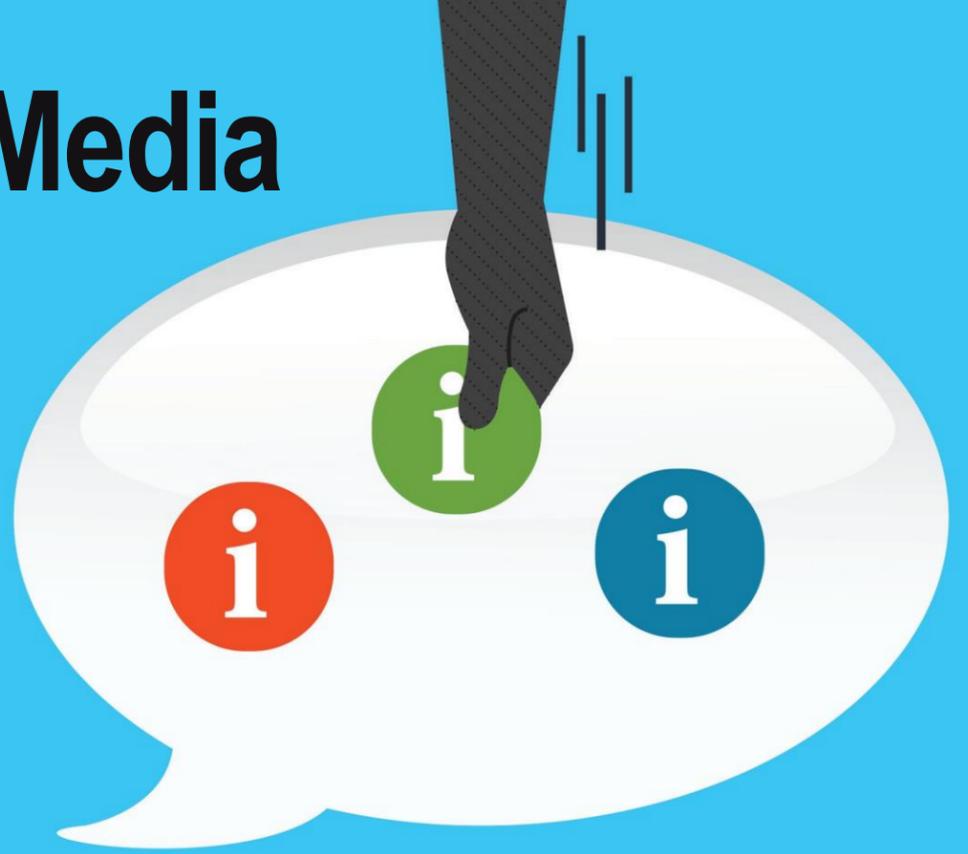


Don't Let Social Media Turn You into an Insider Threat



For many of us, social media has become an essential tool in both our personal and business lives. However, sharing information on social media can be tricky. There really is no way to guarantee the information you share won't end up in the wrong hands.

Sharing on Social Media? Consider These Risks:

Account Security Questions

Security questions rely on personal information that is often shared on social media.

TIP: Turn on Multi-factor Authentication for Accounts

This can lessen the impact of any security questions that become compromised.

TIP: Use and Memorize Fake Information for Security Questions

Try memorizing and using fake answers for hometown, pets, and schools. Use this list when setting up your security questions.

Location Information

It is common to add your location when taking photographs or posts. However, this can give away important information about your business or whereabouts.

TIP: Monitor Your App Settings

Location can give away important information about your organization or whereabouts.

TIP: Wait Until After a Trip to Post

When on vacation, wait until you return to post pictures and travel logs.

Online Support Forums

It can be easy to unintentionally reveal sensitive organizational information, such as a particular product name and version or IP address.

TIP: Be Careful On Online Support Forums

If you are unsure about what is safe to share, check with your IT Department first.

The bottom line for all three areas highlighted in this article is that sharing information on social media can be tricky. There really is no way to guarantee the information you share won't end up in the wrong hands. **So think before you share.**

Remember: Scammers will often utilize phishing campaigns and other scams directing users to sites to download malware.



BANK OF THE WEST
BNP PARIBAS