CLICK THINKING

Quick insights for protecting yourself and your company from online threats

spotlight

SOCIAL MEDIA

Social media has made it easy to stay in touch. However, it's also made it easier for scammers to prey on unsuspecting users.

Social media is part of everyday life.

Yet the same platforms that allow us to connect with family and friends like never before can also harbor risks.

Cybercriminals use social media to seek out potential victims.

Avoid being a target by knowing what to watch for and how to protect yourself.

WHAT YOU NEED TO KNOW TO PROTECT YOURSELF

- Cybercriminals use social media to seek out and track potential targets.
- Platforms like Twitter, Facebook, LinkedIn and others are a perfect smokescreen for scammers.
- Criminals have been known to set up fake storefronts on Twitter to solicit personal information. Always be wary when faced with these types of requests.
- When you post on any platform, remember that cybercriminals can see, too. Don't post anything that might be useful to them.
- Facebook friend requests can harbor cybercriminals pretending to be acquaintances. If you can't verify that the person is who they say they are, delete the request.
- Posts that start with "Did you see these pictures of you..." or "I can't believe what they said about you..." are usually lures designed to get you to click on a link with malicious intent.
- Spend some time understanding the privacy settings of the social media platforms you use. They can be adjusted so only people you connect with can access the information you share.

A PHISHLINE DIGITAL NEWSLETTER PROVIDED BY PHISHLINE LLC © 2017 PHISHLINE, LLC, ALL RIGHTS RESERVED.