online business systems

CYBERSECURITY AWARENESS MONTH

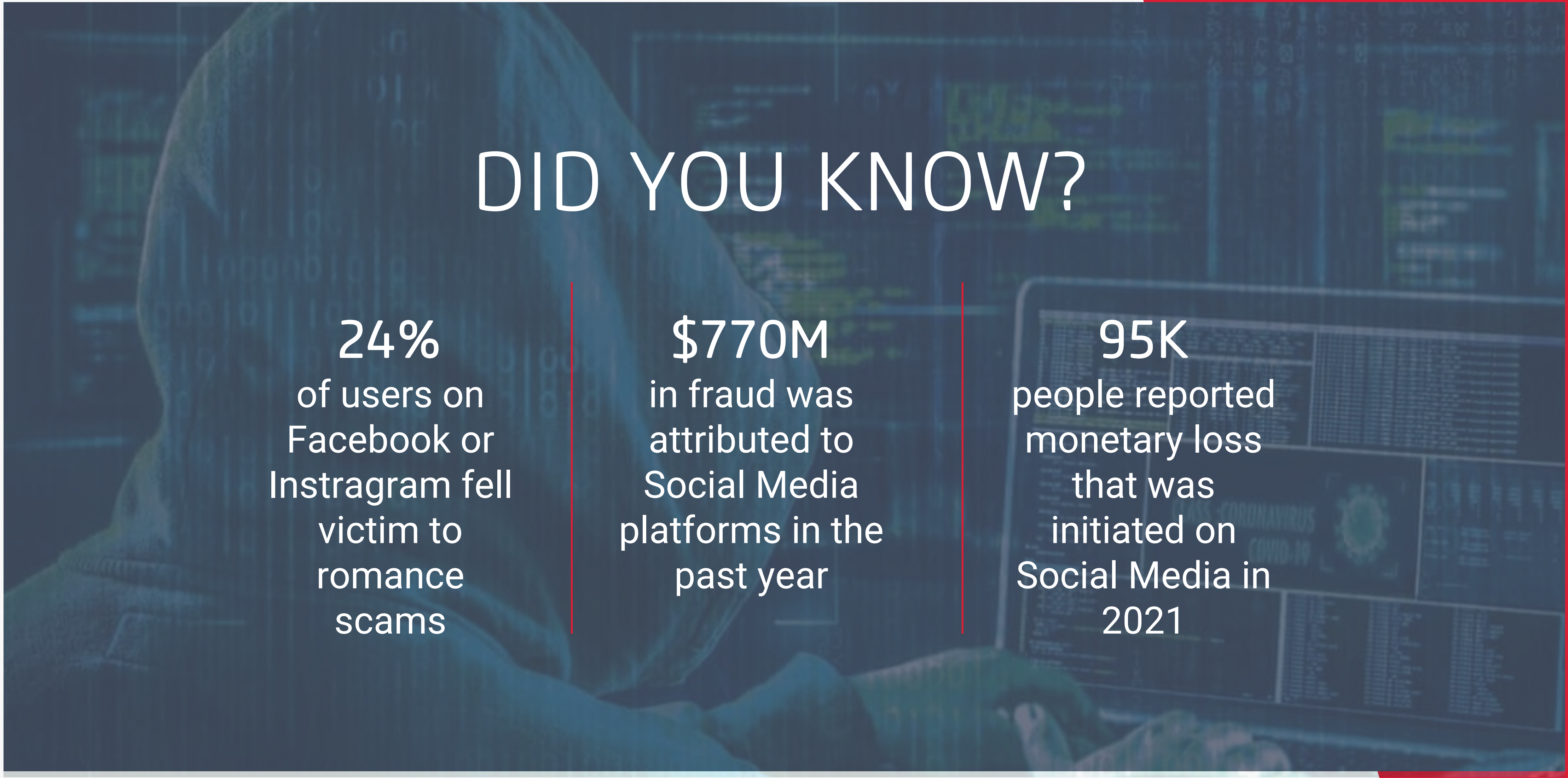
SOCIAL MEDIA DO’s & DON’Ts

October 2022

Results. Guaranteed.

BEWARE THE OVERSHARE

Much has been said about oversharing on social media, be it about your personal life or the personal lives of the people around you like your family, friends, and even children. However, the same applies to your professional life: by oversharing information about your job you are inadvertently putting yourself and your colleagues at risk. Sharing too many photos from your workspace may allow threat actors to get a good lay of the land and make their lives easier if they would want to test your company's physical defenses. Or, with your personal details, adding too much information on social media can make it easier to impersonate you, and commit identity theft.



DID YOU KNOW?

24%
of users on Facebook or Instragram fell victim to romance scams

$770M
in fraud was attributed to Social Media platforms in the past year

95K
people reported monetary loss that was initiated on Social Media in 2021

SOCIAL ENGINEERING YOUR SOCIAL NETWORK

THE FACTS...

- Social engineering is a psychological attack where an attacker tricks you into doing something you should not do through various manipulation techniques.
- Attackers can use Email Tactics, (Phishing), Phone Calls (Vishing), and Text Messaging (Smishing), Social Media, or in Person Tactics.
- Many of us tend to use multiple networking sites, which allows attackers to build a fairly rich profile from information found on these public facing webpages and social networks.

BUT WHY?

- The internet is rife with fraudsters intent on bilking money out of you via all manner of ploys.
- Lurkers are looking for any opportunity to make financial gain, including burglarize your home after you tell the world about your vacation, or active reconnaissance for a bigger ransomware attack found in the corporate party photos your posted.

SOCIAL SHARING

do’s & don’ts

ASSESS YOUR DESK

- Don’t post photos of your personal home or workspace.

- Take a long and hard look at your work desk and remove or cover anything that would be visible in the photo could pose any kind of security risk.

- Consider whiteboards, sticky notes, or any other confidential information that could be captured in a photo.

- Obscuring your images with photo editing software can be reversed if you are not well-versed in using such software.

SHRINK YOUR NETWORK

- Limit and curate what you share on social media – don’t share photos or information that reveals too much about either you, your workplace, or home office.

- Review your social media settings: not everything you do needs to be shared with the wider public, so limit it to people you know and trust.

- Auditing your Facebook privacy settings wouldn’t hurt either. You should apply this advice throughout your online presence, not just to the work-life side.

- Check if you can opt out of targeted advertising.

ALWAYS BE SUSPICIOUS

- If you get a message from a friend about an opportunity or an urgent need for money, call them. Their account may have been hacked – especially if they ask you to pay by cryptocurrency, gift card, or wire transfer.

- If someone appears on your social media and rushes you to start a friendship or romance, slow down. Read about romance scams. And never send money to someone you haven’t met in person.

- Before you buy, check out the company. Search online for its name plus “scam” or “complaint.”

SEARCH YOURSELF ONLINE

What can you find out about your own self?

- Search using multiple browsers, Google, Bing, DuckDuckGo.
- Start by typing your name in quotes, but after that expand your search using the following operators:
  - “FirstName LastName” > What information can I find online about this person
  - “Firstname Lastname@” > Find possible email addresses associated with this person
  - “Firstname lastname” filetype:doc > Any word documents that contain this person’s name
- Search Google Images, Google Maps, and social media sites.
- Learn what other people or organizations have collected, posted, or shared about you online (churches, schools, sports clubs, or other local community sites).
- Understand that these same resources are available to anyone else, including cyber criminals who can use that information to target you.
- For a deeper dive, go to the OSINT Framework https://osintframework.com

online
business systems

THANK YOU

Stay Cyber Safe.