online business systems

SOCIAL MEDIA SAFETY

Do's & Don'ts

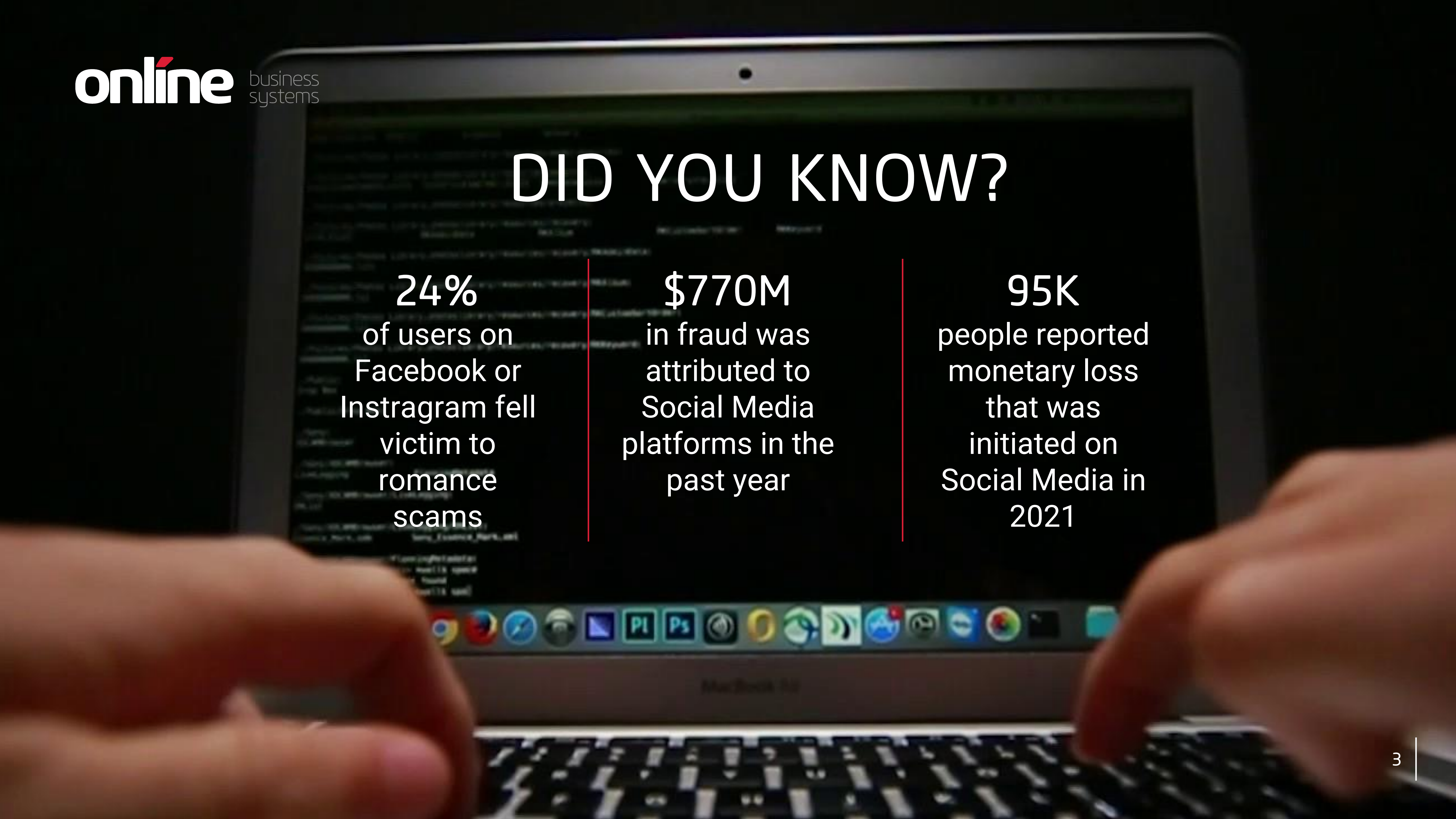
2022

Results. Guaranteed.

BE AWARE, DON’T OVERSHARE

The internet is full of criminals intent on conning you out of your money. Lurkers are looking for any opportunity to make financial gain, including burglarize your home after you tell the world you are on vacation, or active reconnaissance for a bigger ransomware attack found in the corporate event photos your posted.

When sharing photos and information about your personal life, your family, friends, colleagues and details about your professional life, think cautiously and share less. Sharing too many photos from your workspace may allow the bad guys access to information that could lead to a data breach or ransomware. And, adding too many personal details 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

WHAT IS SOCIAL ENGINEERING?

- Social engineering is a psychological attack where an attacker tricks you into doing something you shouldn’t 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.

online business systems

SOCIAL SHARING

do’s & don’ts

5

OFFICE PHOTOS? ASSESS YOUR DESK

- Refrain from posting photos of your personal home or workspace.
- Obscuring your images with photo editing software can be reversed if you are not well-versed in using such software.
- Consider whiteboards, sticky notes, or any other confidential information that could be captured in a photo.
- Remove or cover anything in the frame that may pose any kind of security risk.

ALWAYS BE SUSPICIOUS

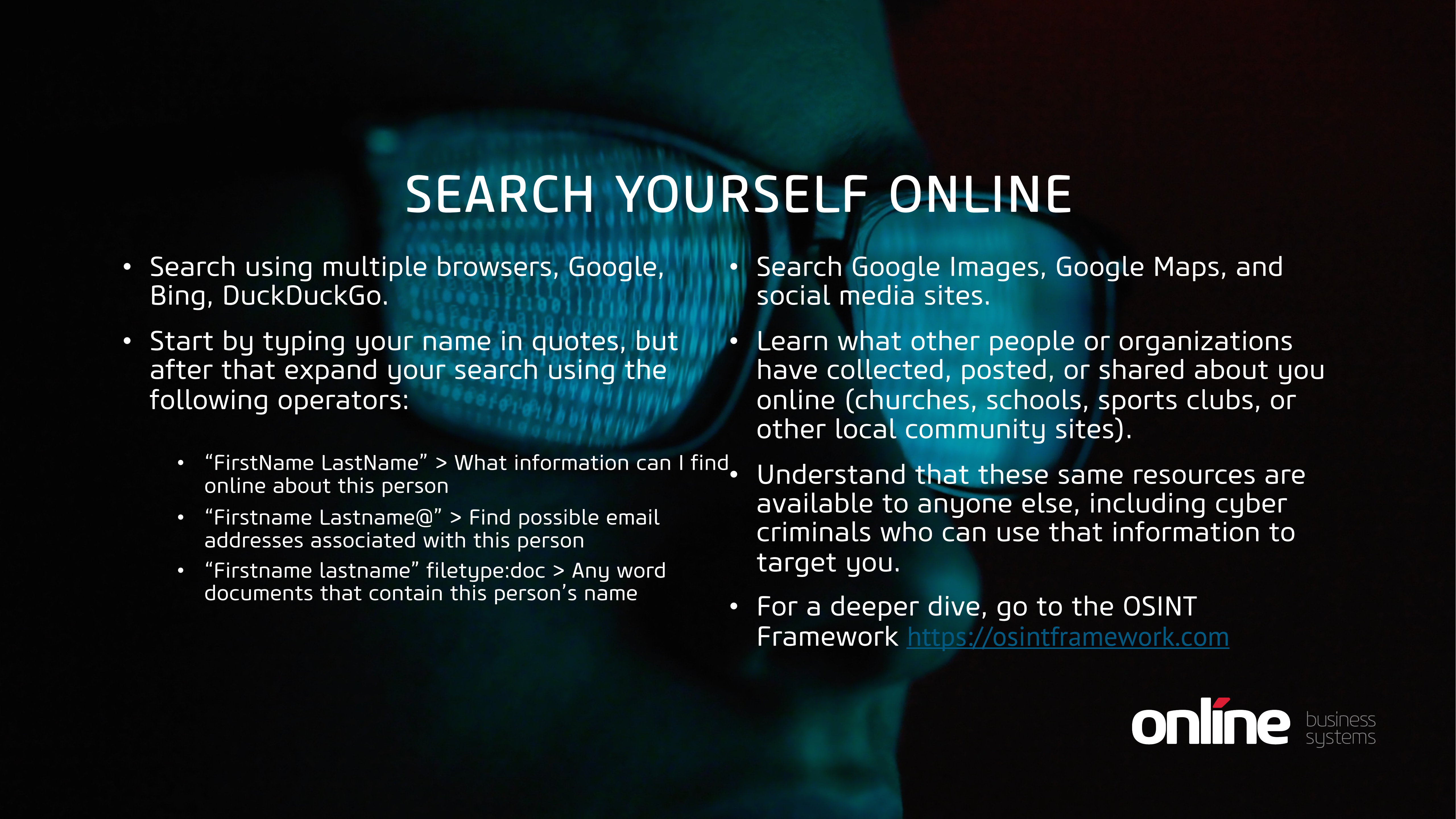
- If you get a message from a friend about an emergency or an urgent need for money, call them. Their account may have been hacked – especially if they ask you to pay by cryptocurrency, gift card, or wire transfer.

- If someone appears on your social media and rushes you to start a friendship or romance, beware. Read about romance scams. And don't send money to someone you haven't met in person.

- If sent a link to purchase something. Don't click. Before you buy, check out the company. Search online for the company name, plus "scam" or "complaint."

SHRINK YOUR NETWORK

- Review your list of 'followers' and 'friends' and purge or block those that you do not recognize.
- Limit what you share on your social media platforms – don't share photos or information that reveals too much about you, your workplace, or home office.
- Review your social media settings and limit your posts to people you know and trust.
- Audit your social media privacy settings, for ALL your apps.
- Opt out of targeted advertising, if possible.



SEARCH YOURSELF ONLINE

- 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

online
business systems

THANK YOU

Stay Cyber Safe.