CYBERCRIME IS ON THE RISE.

HERE'S HOW TO STAY SAFE ONLINE.

STOP

- Don't respond to unexpected pop-ups or messages
- Never click links from unknown senders
- Never give out your Social Security number or banking information

PAUSE & CHECK

- Ask: "Would my bank really email me like this?"
- Pause before reacting to urgent messages or threats
- Talk to a friend, family member, or staff before acting

PROTECT

- Use strong passwords and never share them
- Install updates only when your trusted tech support says it's okay
- Report anything suspicious to your facility director

PROXYWARE

COMMON SCAMS TO AVOID

- Tech support phone calls
- Fake antivirus warnings
- Grandparent scams (*"I'm in trouble, please send money!"*)
- Online romance or sweepstakes promises
- *"We've locked your account"* emails

YOU CAN ALWAYS CALL:

FBI Internet Crime Complaint Center:
1-800-CALL-FBI or www.ic3.gov

FTC Fraud Reporting Line:
1-877-FTC-HELP or reportfraud.ftc.gov

National Elder Fraud Hotline:
1-833-FRAUD-11 (1-833-372-8311)

WANT TO MAKE YOUR SENIOR LIVING COMMUNITY SAFER ONLINE?

Ask your facility manager or local **Attorney General's Office** to bring **Proxyware** to your community.

Proxyware helps protect seniors like you from online scams, fake alerts, and cybercrime.

LEARN MORE OR GET HELP:

proxyware.org/senior (800) xxx-xxxx

help@proxyware.org

PROXYWARE