1. CREATE LONG, UNIQUE PASSWORDS

Length trumps complexity. Strong passwords are at least 12 characters long and include letters, numbers and symbols. Ideally, your password is not recognizable as a word or phrase. And, yes, you should have a unique password for each online account. Sound hard to remember? Using a password manager has never been easier; many smartphones and web browsers include password managers and even suggest strong passwords. Otherwise, we recommend coming up with a password that is actually a "passphrase," that is, a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember, such as *ILov3StayingSafeOnl1ne!* (but don't use that one).

2. THINK BEFORE YOU CLICK

What's the most common way for cybercriminals to get your sensitive information? It's when you click on something you shouldn't have. Malicious links in email, tweets, texts, posts, social media messages and malicious online advertising (known as malvertising) are a direct way for hackers to get your sensitive information. Don't make it easy for them. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Whenever you get an email or message, count to five – usually that's all the time you need to determine if the missive seems authentic or not.

3. REPORT PHISHING

One of the best ways to take down cybercriminals is by reporting phishing attempts, and nowadays its easier than ever. If the email came to your work email address, report it to your IT manager or security team as quickly as possible. If you're at home and

5. SHARE WITH CARE

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.

Source: National Cybersecurity Alliance

Thank you for your attention to these tips which will help enhance your personal and corporate online safety.