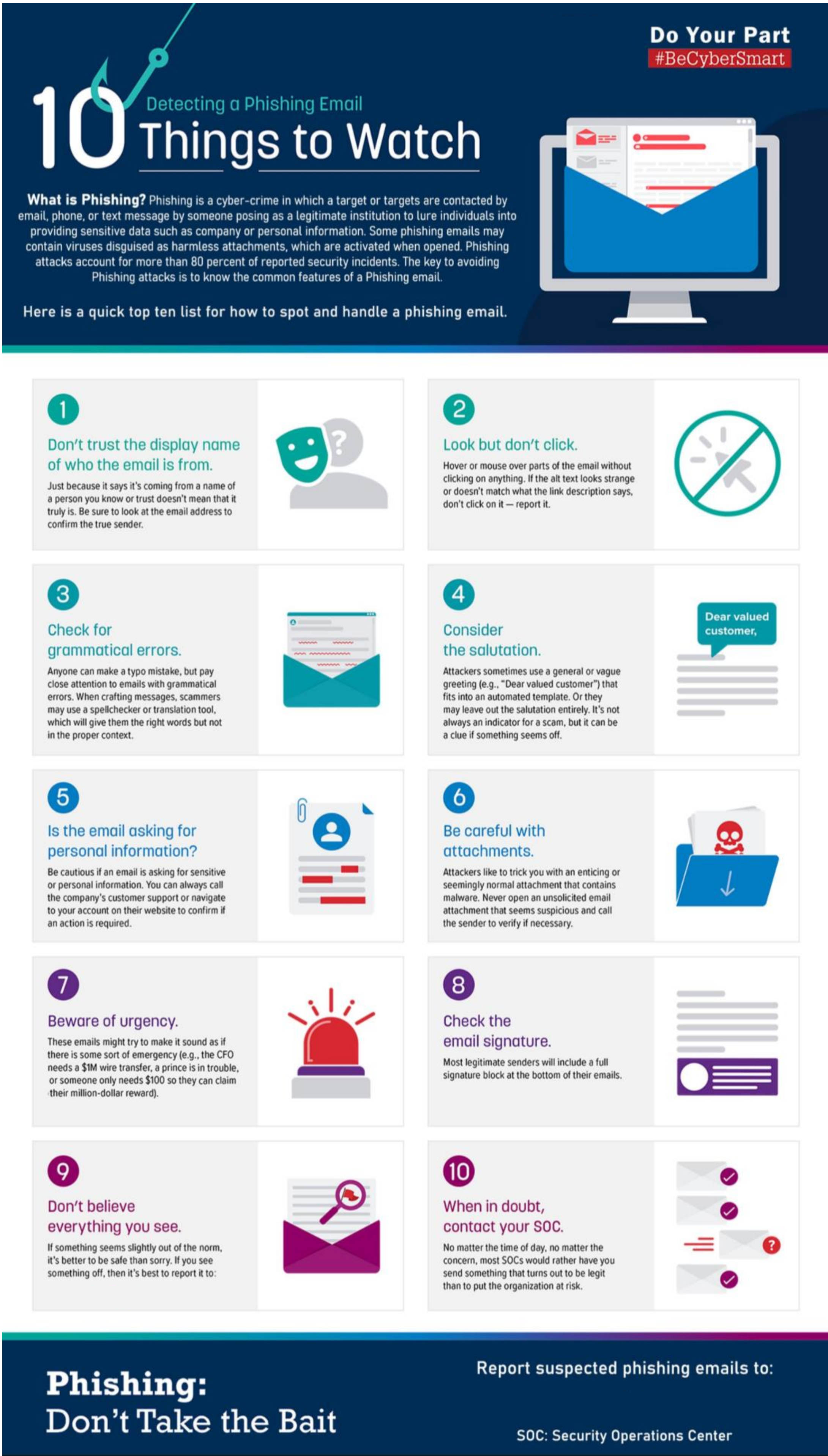
Company identifying information has been removed



Do Your Part
#BeCyberSmart

10 Detecting a Phishing Email Things to Watch

What is Phishing? Phishing is a cyber-crime in which a target or targets are contacted by email, phone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as company or personal information. Some phishing emails may contain viruses disguised as harmless attachments, which are activated when opened. Phishing attacks account for more than 80 percent of reported security incidents. The key to avoiding Phishing attacks is to know the common features of a Phishing email.

Here is a quick top ten list for how to spot and handle a phishing email.

1

Don't trust the display name of who the email is from.

Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look at the email address to confirm the true sender.

2

Look but don't click.

Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it — report it.

3

Check for grammatical errors.

Anyone can make a typo mistake, but pay close attention to emails with grammatical errors. When crafting messages, scammers may use a spellchecker or translation tool, which will give them the right words but not in the proper context.

4

Consider the salutation.

Attackers sometimes use a general or vague greeting (e.g., "Dear valued customer") that fits into an automated template. Or they may leave out the salutation entirely. It's not always an indicator for a scam, but it can be a clue if something seems off.

5

Is the email asking for personal information?

Be cautious if an email is asking for sensitive or personal information. You can always call the company's customer support or navigate to your account on their website to confirm if an action is required.

6

Be careful with attachments.

Attackers like to trick you with an enticing or seemingly normal attachment that contains malware. Never open an unsolicited email attachment that seems suspicious and call the sender to verify if necessary.

7

Beware of urgency.

These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a $1M wire transfer, a prince is in trouble, or someone only needs $100 so they can claim their million-dollar reward).

8

Check the email signature.

Most legitimate senders will include a full signature block at the bottom of their emails.

9

Don't believe everything you see.

If something seems slightly out of the norm, it's better to be safe than sorry. If you see something off, then it's best to report it to:

10

When in doubt, contact your SOC.

No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than to put the organization at risk.

Phishing: Don't Take the Bait

Report suspected phishing emails to:

SOC: Security Operations Center

Company identifying information has been removed

20 TIPS for SECURITY AWARENESS

[redacted]

01 PROTECT YOURSELF & YOUR INFORMATION

Attacks do happen and can happen to anyone.

02 USE STRONG PASSWORDS

A strong password is long; a mix of letters, numbers, and symbols.

03 DON'T "SEE ATTACHED" IN EMAILS

Don't open email attachments you weren't expecting to receive.

04 GET SAVVY ABOUT WIFI

Limit what you do on public WiFi and hotspots because these are not secure.

05 STAY UP TO DATE

Keep your applications up to date on your phone, PC, Tablet and all other devices.

06 SHARE WITH CARE

Think before posting about yourself and others online.

07 PROTECT YOUR SYSTEMS

Use approved enterprise applications.

08 LOCK UP YOUR DEVICES

Lock your phone, computer, and other devices with a secure passcode.

09 SET UP MFA

Enable MFA in any applications that allows MFA like banks, social media, online accounts and enterprise applications at

10 OWN YOUR ONLINE PRESENCE

Configure the privacy and security settings when you download a new app.

11 CLEAN UP YOUR APPS

Remove any apps on your phone you're not using and updating frequently.

12 CONTROL APP ACCESS

Do not install any apps unless they come from the official app store.

13 DRIVE STANDARD PROCESSES

Follow standard business and IT processes and policies.

14 MIND YOUR SURROUNDINGS

Be careful connecting USB devices that you do not know where they came from or cannot confirm the origin. These are common devices are used to introduce malware.

15 BACK UP YOUR DATA

Back up your data frequently.

16 MONITOR ACCOUNT ACTIVITY

Report any suspicious activity on your account to the IT Service Deck.

17 DON'T CLICK LINKS FROM SUSPICIOUS SOURCES

Avoid clicking short links from unknown or questionable sources.

18 BE CAREFUL WITH ONLINE TRANSACTIONS

Be careful before you transfer any money online and make sure you verify the recipient and account information.

19 BEWARE OF SCAMS

Pause before you share your information with anyone offering you something.

20 PARTNER WITH IT

Partner with IT on any new technology solution.

[redacted]