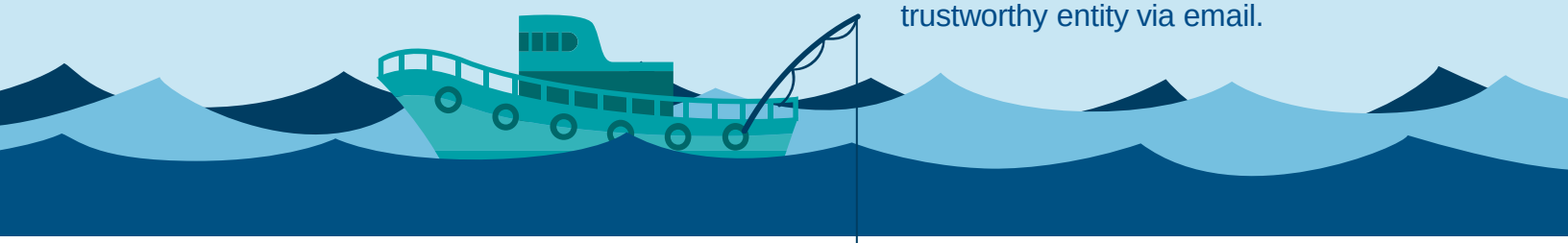
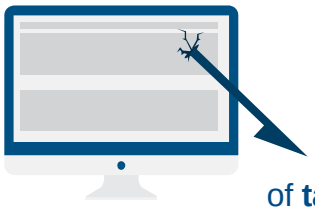
PHISHING

or spear-phishing is an attempt to acquire information, such as usernames, passwords, and company data, by masquerading as a trustworthy entity via email.





71% of **targeted attacks** include spear-phishing(1)

Phishing is the entry point for cyber-attacks(1) **#1**

92.4% of malware is delivered by email via hyperlinks or downloadable content (2)

DON'T GET HOOKED

Look out for **emails**, **calls** and **text messages** that have these characteristics(3):

- Grammar and spelling errors
- Requests to click on links or open attachments
- Sense of urgency
- Appeal to human greed and fear
- Requests for sensitive data

If you ever suspect an email to be phishing **DO NOT** click any links or open attachments.

SPOOFING EMAIL

Criminals use **spoofed** email addresses, usually **one or two letters off** from a company's true domain name

SOCIAL ENGINEERING

Criminals take the time to **understand** your **relationships, activities, interests,** and **travel** or **purchasing** plans in order to gain your trust.

BROWSING PUBLIC INFORMATION

They gather **information** from **social media, websites, and LinkedIn accounts.**

STAY SAFE ONLINE

- Verify sender email address
- Do not enter your username and password into a webpage from a clicked link
- Keep your browser, plugins, and security software up to date
- Verify legitimate URL by checking domain properly
- Do not trust phone numbers found in suspicious email messages
- Use saved bookmark to navigate directly to correct website

TIAA

Sources: (1) Symantec (2) CSO Online (3) Cofense

January 2019