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.

35% Of organizations experience spear phishing\(^1\)

Phishing is the entry point for cyberattacks\(^2\)

96% of phishing attacks arrive by email\(^3\)

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.

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

Browsing public information

Stay Safe online:
- Verify sender email address
- 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
- Do not enter your username and password into a web page from a clicked link
- Keep your browser, plugins and security software up-to-date
- If you ever suspect an email to be phishing, DO NOT click any links or open attachments

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

Sources: \(^1\) Proofpoint \(^2\) IBM \(^3\) Verizon

©2021 Teachers Insurance and Annuity Association of America-College Retirement Equities Fund, 730 Third Avenue, New York, NY 10017