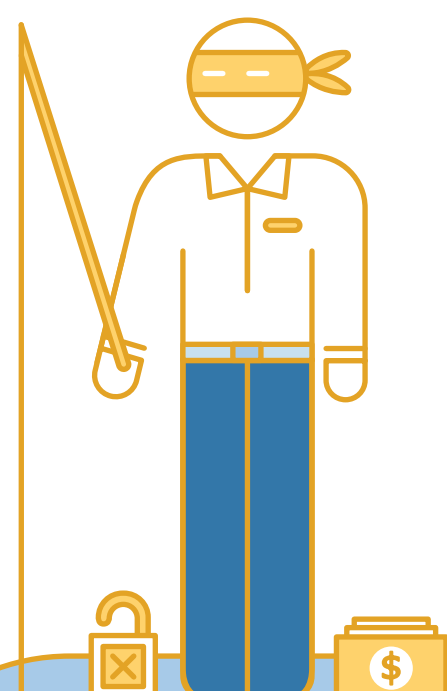


# Spot a phish. Protect your business.

## What is phishing?

Phishing is a technique where cybercriminals send fake emails, texts or websites that look like legitimate correspondence to manipulate employees into gaining access to corporate systems or information.



### Key characteristics:

- Tries to trigger a quick reaction from you
- Provides a link to a separate website
- Typically asks you to "update", "validate" or "confirm" private information
- Often imitates an official sender (e.g. your company or government or financial institution)

91%

of cyber attacks on businesses begin with phishing. <sup>1</sup>

65%

growth in phishing emails occurred over the past year. <sup>2</sup>

97%

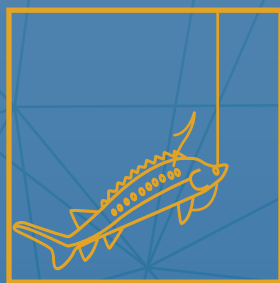
email recipients failed to distinguish a phishing email from a legitimate email in test exercises. <sup>3</sup>

## Types of phishing



### DECEPTIVE PHISHING

Emails targeting all employees that impersonate a recognized / legitimate source that contain malicious links.



### SPEAR PHISHING

Highly personalized emails and fake websites targeting specific employees (e.g. finance).



### WHALING

Highly personalized emails and fake websites targeted to specific senior executives (e.g. CEO).



### BUSINESS EMAIL COMPROMISE (BEC)

Corporate, internal email that impersonates an executive (e.g. CEO).



### PHARMING

Hijacked website domains that redirect visitors to a fraudulent site.

## Think before you click!

What to watch out for.

From: ITsupport2@companyabc.com  
 To: you@abccompany.com  
 Date: July 30, 2018 1:11 AM  
 Subject: Urgent – action required to resolve network issues

Dear Sir/Madam,

Due to recent network issues, we require that all staff log into their profiles to validate their user credentials. Please click here to input your information.

If you do not complete the steps indicated within the next 24 hours, you will be locked out of your account and this will impact business operations.

Thank you,  
 IT Support Team, Company ABC

Unknown / suspicious sender

Sent at unusual time

Sensational/urgent subject line

Generic greeting

Poor grammar and spelling

Contains suspicious links or attachments

Requests personal or sensitive information

High sense of urgency/privacy

Promises a threat or reward

Sender claims to be a person of authority

Talk to your broker about how Sovereign can help protect your business from phishing. [sovereigninsurance.ca](http://sovereigninsurance.ca)



<sup>1</sup> "2016 Enterprise Phishing Susceptibility and Resiliency Report," Cofense. <sup>2</sup> "2017 Enterprise Phishing Resiliency and Defense Report," Cofense. <sup>3</sup> "Intel Security Study," 2015.