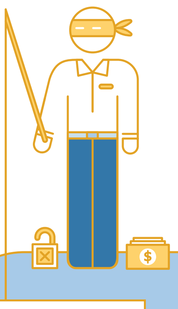
Spot a phish.
Protect your business.

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. [1]

65%
growth in phishing emails occurred over the past year. [2]

97%
email recipients failed to distinguish a phishing email from a legitimate email in test exercises. [3]

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)

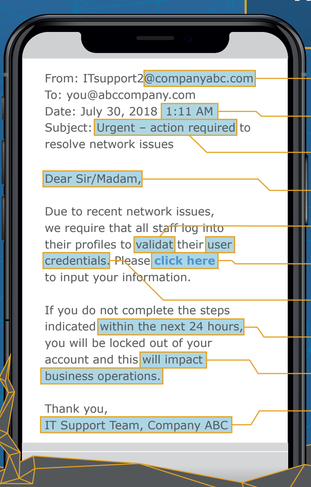
Corporate, internal email that impersonates an executive (e.g. CEO).

PHARMING

Hijacked website domains that redirect visitors to a fraudulent site.

Think before you click!

What to watch out for.



- 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

sovereign® INSURANCE

[1] "2016 Enterprise Phishing Susceptibility and Resiliency Report," Cofense. [2] "2017 Enterprise Phishing Resiliency and Defense Report," Cofense. [3] "Intel Security Study," 2015.