

10 Tips for Detecting Phishing Emails



The Vito Corleone – “Make him an offer he can’t refuse.”

The most common phishing expedition:

- 1) An offer too good to be true (found money)
- 2) An offer so bad it begs a response (your bank balance)

Greetings Gone Bad



If the “To” address AND the greeting are both non-specific - (“Dear friend”, “colleague”, “valued customer”, etc.) - say “goodbye” quickly!

Urgent, Urgent, Emergency!

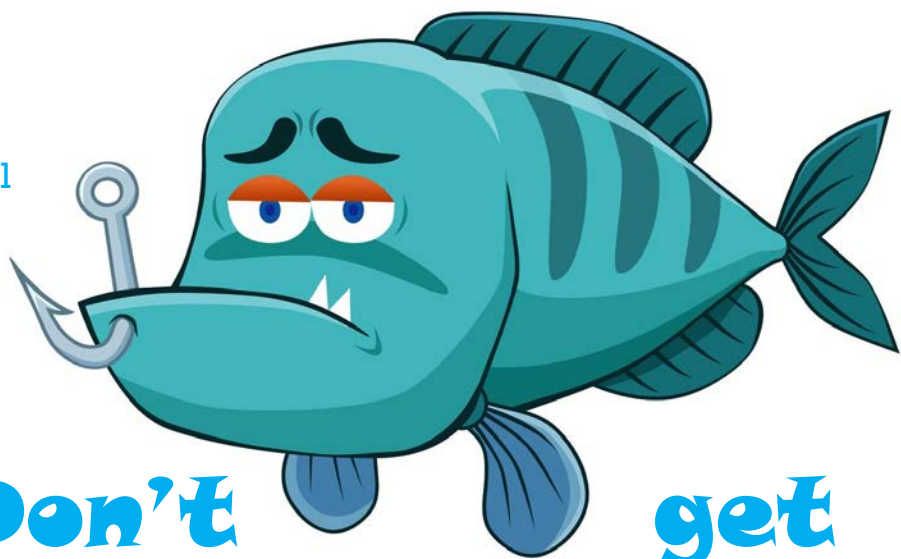


Another central tenet of Social engineering is “Create a sense of urgency”...

Don’t be caught up in the “urgent”.

Your “urgent” response should be to delete it or report it.

Don't get HOOKED



Catch Me If You Can – Frank Abagnale

Beware of emails that include a request for business or personal information ... such as “Update your account immediately.”



Catfish Bite

A catfish employs an email technique called spoofing ... hiding the true “From” – and it’s easy to do!

Always check “From” and use other tips to avoid getting bitten.



Spelling Bee



Simply put, corporations hire the kids who win spelling bees ... hackers not so much!

Poor spelling/grammar is a good indicator that this email is something smelling bad!

Hyper on Hyperlinks

DON'T click on external links unless you check the real address embedded in the hyperlink (hover over the link).



Headers Prevent Headaches!

Headers on an email tell you a history....

File → Properties → Headers
View source - mxtoolbox.com



Phantom of the Opera



“Hide your face so the world will never find you”

Beware files masquerading as other file types, or contained in zips, like...

'exe', 'bat', 'com', 'cmd', 'cpl', 'js', 'jse', 'msi', 'msp', 'mst', 'paf', 'wsh', 'wsf', 'vbs', 'vbe', 'pscl'

This “cheat sheet” is derived from Pivot Point Security’s Cyber Acuity Security Awareness Education offering.

Contact us to see how you can provide thoughtful, interesting, and real-world Security Awareness Training (from security experts) to your employees.

www.PivotPointSecurity.com