10 TIPS FOR DETECTING PHISHING EMAILS

1 THE VITO CORLEONE – "MAKE HIM AN OFFER HE CAN'T REFUSE"

The most common phishing attacks use:

1. An offer too good to be true (free money)
2. An offer so bad it begs a response (frozen assets)

2 THE CUBA GOODING – "SHOW ME THE MONEY"

Money is a foundational element of phishing - attacks will often play on greed.

3 GREETINGS GONE BAD

If the "To" address and the greeting are both non-specific ("friend", "colleague", "valued customer", etc.) - say "goodbye" quickly!

4 URGENT, URGENT, EMERGENCY!

Don't be caught up in the "urgent" - your "urgent" response should be to delete it or report it.

5 THE FRANK ABAGNALE - CATCH ME IF YOU CAN

Beware of emails that include a request for business or personal information ("Update your account immediately.")

6 SPELLING BEE

Poor spelling/grammar is a good indicator the email is phishy!

7 PHANTOM FILES

Beware files masquerading as other file types, like… 'exe', 'bat', 'com', 'cmd', 'cpl', 'js','jse', 'msi', 'msp', 'mst', 'paf', 'wsh','wsf', 'vbs', 'vbe', 'psc1'.

8 CAT-PHISH BITE

A catfish employs an email technique called spoofing … hiding the true "From" – and it's easy to do! Always check "From".

9 HYPER ON HYPERLINKS

Don't click on external links unless you check the real address embedded in the hyperlink - hover over the link.

10 HEADERS PREVENT HEADACHES

Headers on an email tell you a history - if the history looks fishy, delete the phish.

PivotPoint SECURITY

This "cheat sheet" is derived from Pivot Point Security's "Security Awareness Education" program. For more information on how to turn your people from your greatest threat to your greatest threat detection mechanism, reach out! **info@pivotpointsecurity.com**