IT Security – How to evaluate potentially "bad" emails

Email evaluation principles

Email safety principle #1 – Question All Unsolicited emails

Unsolicited vs. Solicited – Unsolicited means **unrequested and unexpected** – even from a known source
Even if you know the sender - if unsolicited, ask, "Is anything unusual about THIS email?"
Unexpected email from "trustworthy" source (UPS, FedEx, banks, retailers, friends, business connections)
Caution – brief emails from "known" persons – Check email address (hover over sender name)
Why? Emails with malware frequently come from a NAME you know – with a different email address.
Evaluate time of day, unusual list of recipients, unusual context or brevity *from this person* ("thought of you")
Any misspellings? Grammar mistakes? Unusual phrasing? Unusual colors? Formatting? Font variations?

General principles for evaluating emails

Antenna up! – Does *anything* seem amiss? STOP – Do you need to click or respond to this now?
Don't get your news from email – Beware news "updates" that show up via email
Beware current events (Olympics, disasters, weather events, holiday messages, celebrity news)
Beware "interesting/insider" product release info (Apple, Tesla, self-driving-vehicles, etc.)
Beware Social media – Popular sites are rife with phishing scams – Don't believe your friends are foolproof
Beware plausible guesses (Your shipment has arrived; Your account needs attention; Resume attached)
Beware "too good to be true?" Does the content make you curious? (Ask, who wants to make me curious?)
Antenna up! Scammers are very intentional in creating elaborate ruses - think twice and be very cautious

Links – Before you click

Do NOT click on links (or open attachments) in emails – unless you know and trust the source
Hover over link, checking spellings, unexpected content, added extensions (amex.us.com) (ups.pickup.com)
Never respond if asked to click link for "confirmation" or "reset", even if they know last 4 of CC#, last 4 of SS#
If you think a request may be legit – instead of clicking link, go to vendor site and login (no copy/paste)
Any "click link" to learn more should result in careful questioning – links can be legit – just be cautious
Think twice – if uncertain contact PBSI or your IT support and ask if this is OK – or (scanURL.net or others)

Recent hacker spoofs

IRS – "you need to reset your Pin#"
Social Security scam – "setup your online account" – to prevent hackers doing so (of course)
Apple account needs renewal – "password change required"
Pokémon Go – Some downloads placed on legitimate third-party websites have been "trojanized"
Game of Thrones illegal download "HBO copyright claim" – pay fee to avoid prosecution…
Gmail alert – You receive text "Google has detected unusual activity." – reset your password
Public WiFi - No passwords - Fake Public WiFi–"Google Starbucks" or "Trump WiFi" (scammed 1,000 @RNC)

This document is intended as a supplement, not a replacement for your own Security Policies & Procedures.

PBSI - Technology and IT Security Solutions

Modified 1/03/2018