PBSI Technology Solutions

www.pbsinet.com

IT Security – How to evaluate dangerous 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)
Check email address (hover over sender name). Caution – brief emails from "known" persons
Why? Emails with malware frequently come from a NAME you know – with a different email address

Safety Principle #2 – Antenna up!

Antenna up! – Does *anything* seem amiss? STOP – Do you need to click or respond to this now?
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?
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

Safety Principle #3 – Don't get your news from email

Don't get your news from email – Beware news "updates" that show up via email. Don't click - use news app.
Beware current events (Olympics, disasters, weather events, holiday messages, celebrity news)
Beware "interesting/insider" product release info (Apple, Tesla, self-driving-vehicles, etc.)

Safety Principle #4 - Careful with Unsubscribe

DON'T: Use "Unsubscribe" unless you are CERTAIN the source is credible
Scammers use "unsubscribe" clicks to 1) confirm your email address is real, and/or 2) initiate an attack
DO: Instead: In Outlook, right click on email and choose, "Junk" then "Block Sender"

Safety Principle #5 – Know how to evaluate a URL for safe Domain name

In any URL, the domain name is the text following the 1st period and before the first single slash
Evaluating the real domain name is key (https://www.exampledomainname.com/moreinfo)
Don't be fooled by links that try to add or misspell trusted domains. (e.Dell.com is NOT Dell.com)

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)
Think twice – if uncertain contact PBSI or your IT support and ask if this is OK – or (scanURL.net or others)

Non-traditional contacts and techniques

Text alerts - You receive text "Google has detected unusual activity." – reset your password – No! Login
Beware Social media – Popular sites are rife with phishing scams – Don't believe your friends are foolproof
Phone calls – Never give personal info or cc info to a phone caller. Phone "vishing" scams are increasing

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