ANATOMY OF A PHISH

Employees receive a **LOT** of email. Despite the effectiveness of spam filters, users still need to be on the lookout for malicious emails and understand the various types of attacks we may see as criminals attempt to gain access to sensitive information.

What to watch out for

- **Eye catchers** – "You WON!," "Great deal!," and other attention grabbing headlines including many of the fake news sites that popped up over the last year can indicate a phish as they appeal to the curiosity of the recipient and the desire for a good deal.

- **Unusual requests for information** – Either from unknown sources asking for information they shouldn't have access to, or inquiries from friends/family about things they should already know

- **Urgency** – "Limited time only!" and "I need you to bail me out!" messages create a sense of pressure to react quickly. If truly urgent, email likely wouldn't be the channel.

- **Messages with links or attachments** –Particularly if from an unknown sender, but even from a friend, have a healthy suspicion of links and attachments. Hover over links to see where they go, and look at whether the attachment has an "x" or "m" at the end (.docx, .pptm) which indicate an executable file or a file with macros, both of which can install malware on your system. View with caution and check with the sender if you weren't expecting it.

- **Misspellings** – Especially in the "From" line, pay attention to the email address and whether it's correct (ex. Smith@companyname.com vs. John.Smith@companyname.com). Easy to miss, but an important distinction that could keep you from sending information to an attacker. Misspelled words in the body of the email can also be a clue, as most people use spellcheck.

- **Communications referencing government agencies** (IRS, District Courts, etc.) – Governmental agencies generally will not reach out via email for action; they will send a hardcopy letter. Any communications referencing these agencies and requesting quick action should be looked at with suspicion and verified via alternate means.

DIFFERENT TYPES OF PHISHING

Type of Attack	Targeted Victim	Description
Phishing	Any employee	• A targeted individual is contacted by email or telephone by someone posing as a legitimate institution to lure the individual into providing sensitive information such as banking, credit card or password details. • Usually sent in bulk distribution and not personalized to the recipient (ex. Starts “Dear Customer”)
Spear Phishing	Employees with access to sensitive data (ex. customer databases, financial transactions)	• More targeted and sophisticated than phishing, uses personalized information about the victim gained through public sources (ex. social media posts) to appear to be from a trusted colleague, friend, family, bank, etc. • Victims are targeted based on access with the goal of gaining access to systems or carrying out financial transactions such as a money wire
Whaling (a.k.a. Business Email Compromise or BEC)	CEO or other high ranking company official	• Victim is targeted with the goal of gaining access to sensitive non-public information or to pose as the victim and entice employees to provide access based on the victim’s request • Access to the victim’s profile may be gained through spear phishing attacks

One big mistake users make is thinking “it could never happen to me, I don’t have enough money, data, or don’t work in a target company” – WRONG! Particularly with traditional phishing attacks, none of this matters. Attackers send out hundreds of emails at a time looking for that one person who’s going to click, basically looking for a quick payout. There are even subscription services criminals can use where they pay a monthly fee and have access to tools that enable them to send hundreds of thousands of phishing emails.

Best first step: Slow down and take a second look

No matter how much we've learned about phishing, it's still easy to get hooked. You get busy, and in the midst of a flurry of emails, see an email that seems familiar, and take the bait. So remember this: When it comes to phishing in all forms – including fraudulent phone calls – the best first step is to pause and think before taking action. Slow down and evaluate the information. You may find it easier to recognize some of these triggers and avoid being caught in the trap.