JFX, LLC
Cybersecurity Consulting

Cybersecurity Briefing: Phishing and BEC Emails

Phishing emails are designed to deceive recipients, and are a cheap, effective way for hackers to gather confidential data, scam money, or distribute malware. Billions of phishing emails are sent daily, usually in mass emailings. Attacks that target a person, group or organization are called ‘spear phishing’. Over 99% of phishing emails are blocked by general email (Outlook, Gmail) or specialized email filters (Proofpoint), but filters are not perfect and sometimes phishing emails arrive in your Inbox.

Business Email Compromise (BEC) is a type of spear phishing attack which impersonates a known sender and targets specific individuals, often incorporating accurate information for credibility. Common BEC attacks request changes to payment instructions, ask for confidential information (*CEO: ‘pls send employee comp info for bonus calcs’)*, or the popular scam: ‘*please buy gift cards and send me the redemption codes*’. BEC emails can come from compromised email accounts, making them even harder to detect. BEC attacks are especially challenging around holidays when distractions make them less likely to be noticed, e.g., with key individuals away and others covering their jobs.

While some phishing emails have spelling errors or confused writing, others look legitimate and can be very hard to identify. Here are some key things to consider when you get an email, text message or other communication that could be a phishing or BEC attempt.

Is the message one you expect to receive?

Effective phishing emails seem plausible and mimic legitimate messages, e.g., an Amazon delayed delivery notice. Hackers use subjects to grab your attention. To create a sense of urgency, phishing hooks often play on fear (‘your account is overdue’) or greed (‘your gift card is about to expire’). Be cautious, especially with unexpected messages, and consider other ways to confirm their legitimacy, e.g., check delivery status via your Amazon account.

Does the sender’s email address match the displayed name?

It is easy to spoof a sender’s displayed name (“Joe Smith”), but harder to fake the email address (JS1986@gmail.com). Some email systems display both automatically, others just display the sender’s name and you need to hold a cursor over the name or hit Reply to see the sender's email address. Check. *Why is a business notice from a Gmail account…?*

Does the website address match the displayed name?

Similar to the name / email address mis-match, it is easy to spoof a website’s displayed name that does not match the address of a link. On most browsers, hold your cursor over a link to display its actual address in the lower left corner of your browser window.

Reminder: urls and website addresses anchor to the right.

Make sure that *what is to the right is right*. Secure.chase.com is a Chase.com site; chase.secure.com isn't. Amazon.deliveryupdates.com is not an Amazon.com site.

Does the email or website address have a minor spelling error?

It is cheap to register a website or email domain with a name similar to a real site or company. Some people won't notice @chasse.com rather than @chase.com, or chase.biz instead of .com. Get in the habit of checking those details. If in doubt, open a new browser and access a site directly or via Google rather than using a provided link.

If you are curious, you can check information about a domain address at the internet organization www.ICANN.org, . As one hint for suspicion, was the domain created recently?

As a protective measure, many companies register domains similar to their own to prevent hackers or competitors buying and mis-using them, e.g., www.amazone.com is registered by Amazon. Consider registering domains similar to your business name so others can't.

Is the content style reasonable from the sender?

Greetings and writing styles can be impersonated, but consider if the message is written as you'd expect from that sender. "Dear Employee" versus "yo team"? "Hi Elizabeth" or "Hi Liz"? Emojis from the CEO? Unusual styles are clues of impersonation.

Is the requested action usual and reasonable from the sender?

Fraud requests often create a sense of urgency ('for a big client', 'before I leave on vacation', 'pay immediately or …'). Unexpected requests should be treated with caution, especially if they demand immediate or unusual action. If in doubt, double check with the sender - and call or text for confirmation. (Replying to a compromised email just lets the hacker tell you 'Yes, my request is legit'.)

Be careful with requests for financial information

For personal emails, always be careful if asked for your social security number or financial information, even if it is to send you money. A common pattern: 'we will send you $$', the follow-up asks for SSN or bank account details, then a demand to pre-pay or re-pay money.

Verify all requests to change payment instructions, e.g., to a new bank account

Companies should have procedures to verify payment instructions; do not just accept changes provided in the payment request or invoice. Tell companies how to verify changes to your payment instructions, to avoid 'we already paid you, in bitcoin - like you asked'. If in doubt, call using contact info you already have (not listed on a potential fake request).

JFX, LLC, is a cybersecurity consulting firm. To learn more email john.falck@jfxllc.com