5 TIPS FOR AVOIDING SPEAR PHISHING

BOTTOM LINE:

Vigilance Is Key

It may seem like an inconvenience to do a little extra homework or research to confirm emails are legitimate, but it's essential you know who you're dealing with. Without the legwork, you are taking chances and putting yourself and your company at significant risk. High-profile spear phishing breaches are forcing companies to be proactive about identifying the weakest links in their security. Don't be one of them

Spear Phishing emails are more sophisticated & look more legitimate

Phishing emails have long been employed by scammers to trick unsuspecting users. But these catch-all communications are often clumsy attempts to gain information and can be relatively easy to spot. More difficult to recognize are "spear phishing" attacks, which are developed by scammers to target specific companies or even specific individuals.

Because scammers take more time and effort to focus in on their targets, spear phishing emails are more sophisticated and look more like legitimate communications. Top corporations, high-level executives, and media outlets like the Associated Press and Twitter have all fallen victim to spear phishing attacks. And the attacks are only becoming more and more frequent.

As many news reports on these attacks have stated, educating employees and conditioning responses and actions is essential. **Following are five tips all individuals can use to safely manage their emails:**

1. Be cautious. PERIOD.

The main point is you shouldn't automatically trust any email message. Familiar logos … familiar senders … familiar personal information … none of these is an indicator of a safe message. Don't be lulled into a false sense of security.

2. Don't provide any personal information publicly on social networking sites.

Scammers troll the internet for information they can use to make their communications seem more legitimate. Information such as birthdays, anniversaries, and the names and ages of your kids are valuable pieces of data for scammers. Limit the personal data you share with strangers and don't assume an email that includes your personal information is genuine.

3. Do your research on emails that request immediate action.

Even if an email seems to come from a company you trust, do your due diligence before clicking a link or calling a number in the message. To be safe, make contact through a company's website or use a known, verified phone number. Scammers use masked links and false phone numbers to trick you.

4. Be wary of emails that use popular topics or celebrity gossip.

Scammers know that people are interested in celebrity news and scandals and up-to-the-minute sports coverage, and they use those kinds of topics to make their emails seem more interesting. Rather than clicking URLs or images in random emails, find your news on reputable, familiar sites.

5. Be certain of attachments before downloading.

As noted, just because an email is from a friend or colleague doesn't mean it's safe. Cybercriminals can easily collect email addresses from online sources and send an email that looks legitimate. When you receive unexpected links or attachments from friends or colleagues, it's best to verify they actually sent you what you received.

CYBERSECURITY HEROES

proofpoint.