Beware Of That Linkedin Invitation It Could Be A Scam

Of all of the schemes deployed by hackers and cybercriminals, phishing has to be the most effective, pervasive, and dangerous. It relies on tricking users into willingly giving up their login information, and has led to numerous cases of identity theft and data loss. It's even at the core of many cases of corporate espionage and election interference — which goes to show that even some of the most powerful entities on Earth aren't completely immune to the tactic.

That said, researchers are constantly probing the most common phishing techniques in order to help businesses and individuals protect themselves more effectively. After observing phishing efforts for several months, a cybersecurity training organization came to the conclusion that over half of the phishing emails are targeting one social network in particular: LinkedIn.

Of all of the social networks on the web, why is LinkedIn singled out as a hotbed of phishing activity? Why not Facebook — the most popular network of all? Well, believe it or not, there's a good reason why LinkedIn is a prime focus for cybercriminals, and we'll be breaking down why you should think twice before clicking any email invitations to join someone's LinkedIn network.

Hotspot, target, or both?

KnowBe4, a popular cybersecurity and phishing defense training firm, recently compiled a substantial report on phishing attacks and techniques during the second quarter of 2019. According to their findings, LinkedIn accounted for 56% of all phishing email subject lines.

This means that more than half of the phishing attempts (which are up 75% compared to last year at this time) tried to hijack the LinkedIn logins of the users they targeted.

These phishing emails typically take the form of an invitation, where another LinkedIn user invites the victim to “join their network on LinkedIn.” This is the normal method that LinkedIn allows for networking, so the tactic can easily fly under the radar for the uninitiated.

Once a victim clicks on the spoofed link found inside the phishing email, they’ll be asked to log into LinkedIn — but the login fields aren’t real. Instead, the page captures the username and password the victim inputs, and saves it to a database for exploitation (and possibly to sell on the dark web).

Because of how routine the entire operation can feel, the scourge of phishing is often under-reported and highly effective.**Kim Komando, excerpt posted on SouthFloridaReporter.com, July 29, 2019**