FACT SHEET
U.S. Army Cyber Command

The Nation's Army in Cyberspace

www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

THE FACTS: LINKEDIN SCAMS

LinkedIn is a great resource for job searches and building professional connections, but it's not immune from scams and malicious activity. In fact, because the platform and the connections to be made there tend to be more trusted by users, it is commonly used by criminals and hackers for profit, to spread malware, or to steal personal or sensitive data.

What are some common LinkedIn scams, and how can I protect myself against them?

-- **Fake invitations.** These are fraudulent emails inviting you to connect with another LinkedIn member that could be a way to deliver malware designed to steal your information. These can be generic invitation requests or may disguise themselves as romantic approaches. It's always wise to be cautious about clicking on suspicious links in any email, and you should never respond to a connection request in an email. Instead, use the LinkedIn platform and log into your account to check your connection requests.

-- **Phony job offers.** These are LinkedIn messages that claim to be from job recruiters with a great job to offer you, often one that will pay big money and allow you to work online. The offers frequently have links to sites asking you to fill out an application, upload a resume, provide personal information such as a Social Security number, or make a payment. Use caution and do independent research to determine if the sender, organization and offer are legitimate before sending any money or information.

-- **Phishing.** These scams use a variety of methods to tempt users into clicking on links in emails and messages that are designed to help a thief steal LinkedIn users' information. User profiles offer a wide variety of information scammers can use to steal personal data, access sensitive organization information, and launch targeted "spearphishing" against specific individuals or "whaling" attacks against senior members of an organization. More than one source has named bogus LinkedIn invitations as the most common phishing or spearphishing tactic, and security clearance holders are often targeted and need to be particularly vigilant. Again, the best defense is to protect your data and credentials by treating questionable emails and messages with caution, and not clicking suspicious links or opening unknown attachments.

ABOUT US: U.S. Army Cyber Command integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries.

As of 24 September 2019

-- **Tech support impersonation.** Scammers have posed as LinkedIn technicians, often warning that a member's account is in danger, to trick people into clicking on malicious links, or offered LinkedIn technical support by phone for a fee. In a recent tripwire article LinkedIn support staff said they do not charge for customer support, offer no customer support phone number, and will never ask for passwords or access to a user's computer. LinkedIn's phishing information page adds that legitimate emails from LinkedIn are digitally signed for protection and include a security footer to help verify their authenticity. Again, users should take care when confronted with suspicious links or third-party sites offering LinkedIn assistance.
-- **Inheritance scams.** These scams that have been around for years involve emails or messages that claim a LinkedIn member is due a large inheritance, and can claim it by paying the sender a processing fee. Users who get these "advanced fee" scam messages in LinkedIn should not reply, and report the messages to the platform by clicking the "more" icon (…) at the top of the message and selecting "Report."

How can I tell if a profile is fake?

Scammers often create fake LinkedIn profiles to support their illicit activity. These phonies can be pretty sophisticated, and might even indicate that at least one of your authentic LinkedIn connections has accepted an invitation to connect with them. While it doesn't guarantee they are fakes, you can detect potentially sham social media profiles by watching for:

-- **Bogus photos** that are of exceptionally good quality or images of (often lesser) known public figures. One way to check a photo's authenticity is to use a search engine to do a reverse image search that will tell you where the image is being used online.
-- Incomplete profiles that have little to no real information about the person profiled, or have generic job titles such as "manager".
-- **Few connections,** connections that are all the same gender or have fake-looking profile photos, or a lack of connections at the organization listed in the profile.
-- **Fake names** that are common or generic, or the names of (often lesser) known characters or public figures.
-- **Poor or unusual spelling** and poor grammar.

-- **Suspicious work history:** For example, Jane's profile says she is a top Ivy League graduate, but her work experience doesn't support those credentials. If you're suspicious about a person, look elsewhere online for information on the current employer listed in the profile and contact them to check it out.
-- **Suspicious companies:** As with questionable work history, do a search and check it out – does the company exist, and is it what the profile says it is?
-- **Little content** or updates and little to no engagement with other users

ABOUT US: U.S. Army Cyber Command integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries.

As of 24 September 2019