BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

June 2016 | Briefing 19

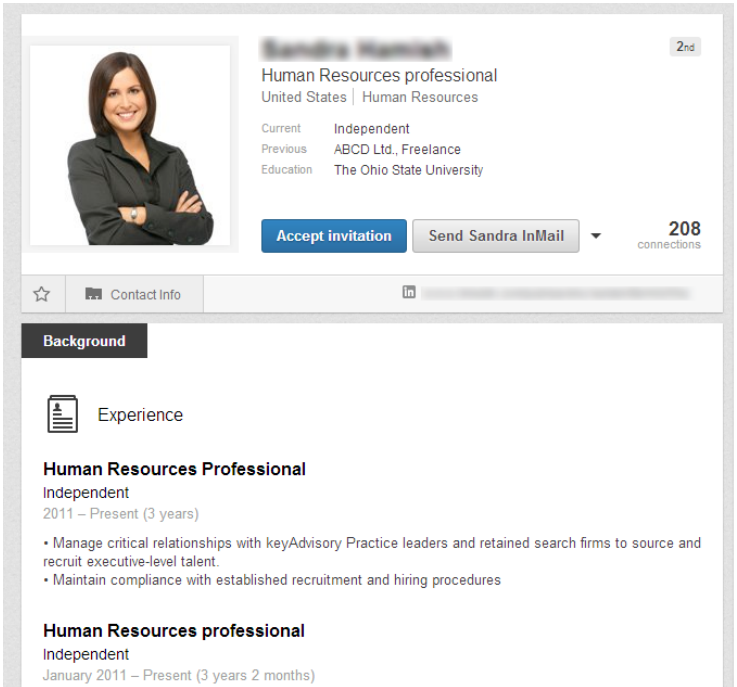
LINKEDIN....BUT TO WHO??

Face it, if you're a professional, you probably have a LinkedIn profile. You use it to catalog your career, maintain professional relationships, stay current on business-related topics and search for new employees or new opportunities. LinkedIn has become a standard, almost required tool for today's professional.

But as LinkedIn has become more and more established as a professional networking site, it has also become an environment where cyber criminals are active. **What do the criminals want? They want to connect to you and your network of contacts.**

HOW DO THEY DO IT?

1. **Some of the most effective LinkedIn scams features cyber criminals who are posing as a recruiter or an executive recruiter.** They create scores of recruiter profiles, carefully created to score well against LinkedIn's searching algorithms. For example, a profile targeting software engineers would contain a job history or professional credits which many related keywords, such as development languages and engineering methodologies; while one targeting HR would contain the names of typical HR regulations and requirements. Most of the time, they contain blocks of language lifted from other "legitimate" profiles When job seekers find these profiles, they often link to them. The more connections, the more credible the profile seems.



IT'S NOT JUST LINKEDIN

Social Engineering reconnaissance is not limited to LinkedIn, not by a long shot. Facebook, Google +, Snap Chat, even dating sites, are plagued with fake profiles created by scammers who seek to build networks of connections. The more connections they make, the more groups they join, the more legitimate the profile seems. Remember, gathering connections is the first part of the scam. Eventually the scammer will try to leverage the connections they have gathered.

2. **A second, common tactic is for the scammer creating a completely fictitious profile, created by a fake company employee.** The bad guys will mine legitimate profiles for keywords, job titles, project names, to build out a fake employee profile that looks convincing. The fake profile will be impressive, with publications, speaking credits, and professional credits lifted directly from real individuals. The scammers will use the fake profile to reach out to other people, via directly inviting them to connect, or through an InMail campaign. Posing as a company employee, the scammers find it easy to link to other company employees, or to peers at other companies.

3. **The third basic tactic is for the scammer to actually create a duplicate profile for an existing person.** If you have ever gotten a request to link in from someone you think you are already connected to, it's likely that the request is coming from a masquerading account. The bogus account will look real – it will probably carry a copy of the photo from the appropriated account. The bad guys are literally assuming the identity an existing person, then trying to quickly build up their social engineering network from the real friends of the real account holder.

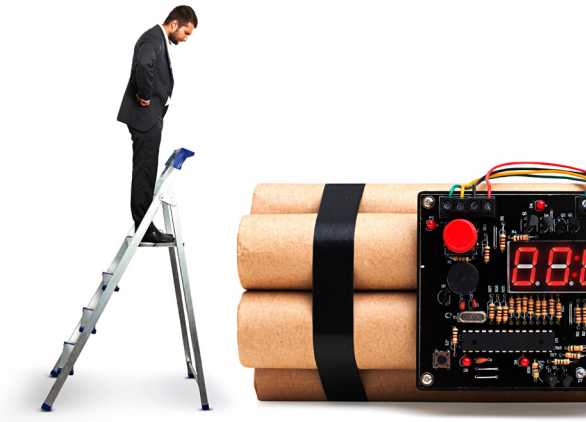
HOW DO THE CRIMINALS USE THESE ACCOUNTS?

Most of the time, bogus accounts are used to gather social engineering information about work groups, including reporting relationships, and current projects. In addition, as the criminals add connections to their masquerading accounts, they gain credibility, making it easier for them to add connections more quickly.

These connections provide the scammers with easy access to you and your peers. They will use this access to explore your network, and to build up relationships. When they have amassed enough data about you and your workplace, or you and your network, they will launch an email based attack. And because they have invested in becoming part of your network, **the attack will come from a sender you thought you could trust.**

ATTACKS COME IN ALL SHAPES AND SIZES

In the simplest attack – targeted at you, the email will contain a request for help – your "contact" will send you InMail, asking you to review a new version of their resume, or to read and comment on the draft of a pulse piece. The email will contain a link, or perhaps the email will contain an attachment. It won't matter. **If you click on the link or open the attachment, your system will be instantly infected with malware, ransomware or both.** What's worse, the malicious payload might contain multiple attacks, which will launch at different times in the future.



A more sophisticated attack is the BEC attack – this attack leverages the network of your colleagues that the scammers have mined from your personal contacts, and the contacts of your peers. **In the BEC attack, the email will appear to originate from a superior at your work, and it will be delivered to your work colleagues.** The email domain will look like your regular work domain. The email will contain a link, an attachment or both. If you click, the end result will be system infection or a larger scale network lockout.

The most damaging of these kinds of attacks are called "whaling attacks". These are almost always targeted to the finance department or another team that directly controls valuable assets. With astonishing accuracy and detail the criminals will use the social engineering data that they have carefully mined to create a plausible (and urgent) request for important company assets to be sent to a third party. Most often the request is for cash (to pay a partner, or to initiate an important deal), but sometimes the request is for other intellectual property – such as a copy of a sensitive contract or a collection of personnel records. **These whaling attacks usually strike late in the week, perhaps before a holiday weekend, adding to the urgency of the request.**

WHAT SHOULD YOU DO – THREE EASY STEPS TO SAFETY

1. On any professional or social network site, when a stranger ask you to connect online, be careful. As yourself, how do I know them? Do we have any common connections? Do we have many common connections? It is so easy to ask a friend to verify that they know the individual asking you to connect. **Only connect to people you are confident of.**

2. When a friend or colleague asks you to link online, be just as careful – were you linked to them before? Review the profile with suspicion. Does the job history of your "friend" make sense? How many connections does it have? Are they connections that make sense. Search for your friend's actual profile. It's highly likely that you are being approached by a scammer who masquerading as your friend. **If you are suspicious, report the profile to the site.**

3. Finally, whenever you receive an email from someone asking you to review and attachment, follow a link, or take an action (including wiring money somewhere!), ask yourself: "Is this an email that I expect, from a source that I trust?" The more urgency you detect in the email, or the stranger the story, the more your threat radar should activate. Make a call, ask a friend what they think. **Before you click, take steps to independently verify the legitimacy of the request.**

WHAT SHOULD YOUR BUSINESS DO?

Social Domain Fraud and Social Masquerading are common techniques used by cyber criminals. But if your company's security team monitors for unauthorized social domains or profile activity, unauthorized pages and masquerading profiles can be take down before they can gather too much organizational information. Even authorized affinity groups and interest groups can be a problem. They are sometimes organized by the scammers, as way to harvest lots of connections quickly. Monitor for those too, and when you find them, stop them.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.