# The Small Business Impact of Social Engineering

by Jeff Berwick

*July 1, 2017*

These days it's impossible to ignore the deluge of cybercrimes and the subsequent media coverage that follows. Ransomware, like WannaCry and Petya, are the largest and latest attacks to dominate the 24 hour news cycle. They use NSA grade exploits to target millions of machines around the world, but they're nothing new. Thousands of smaller scale attacks happen every day, without getting the same media attention. Think of every potentially threatening spam email that you've seen in your work inbox alone. These types of attacks may be even more damaging to businesses than their larger counterparts, because they are so common.

When you put yourself in the shoes of a cybercriminal it doesn't take long to realize that the most vulnerable network in your company is the social one between your employees and the outside world. Social engineering attacks, like spear phishing emails, are the biggest bang for your bitcoin, and often the most difficult to defend against. With a little bit of research and a well-placed email or phone call, a malicious actor can have the keys to the kingdom in no time. It doesn't take any special skills or expensive equipment to manipulate someone into divulging confidential information, which is why it's important to educate your employees on the threats we often take for granted.

In 2015 Ubiquiti Networks, an IT hardware manufacturer, transferred $46 million dollars in a wire transfer scam that was designed to look like it came from someone internally. It was surprisingly unsophisticated, but incredibly devastating, and it can be scaled down to any size. Security Researcher, Brian Krebs, has written a lot on this subject in "Spoofing the Boss Turns Thieves a Tidy Profit". Oregon businesses aren't immune either. There have been more than 50 reported breaches in Oregon this year alone.

Cybersecurity is an arms race between those that protect us and those looking to exploit us. It's an environment that changes so rapidly that business need to be thinking about how to protect themselves, if they aren't already. There are a variety of steps you can take to keep from becoming a victim. Proper email filtering, a well-tuned firewall, and advanced malware protection are just a few options, but a well trained workforce is just as important. Knowledge can drastically improve bad end user behavior. It's no longer acceptable to tell yourself that "some people just aren't technical." Empowering your employees with security awareness training is good for business, and they may even be able to save themselves with it one day.

At Portland Internetworks we like to sleep at night. Our layered approach to cybersecurity is easily replicable and proven to reduce or isolate social engineering attempts. Each layer acts like filter, right down to your workforce, until there's nothing left to get through. We're happy to chat with you about the tools we use. We'll even develop a custom solution that fits the size and needs of your company. Call or contact us for an estimate, but don't wait to start the conversation after it's too late.