Written by Tiana Lopez, Marketing Coordinator
Mode5

Email scammers are constantly looking for ways that they can steal your information, infect your devices, and convince you to sign up for the "next best thing". The most recent example of this is the Google email scam that swept all over the internet and social media. Thankfully, the alert to Google was made rather quickly to disable this activity, however there was quite a bit of damage already done. According to an article written by Alex Johnson with CNBC, "Google said it had "disabled" the malicious accounts and pushed updates to all users. The vulnerability was exposed for only about one hour, and a spokesperson told NBC News on Wednesday night that it affected "fewer than 0.1 percent of Gmail users" — which would still be about 1 million." -Alex Johnson, CNBC, May 4, 2017.

One million users are a lot. Can you imagine that level of damage being done to the users in your business? If you find yourself using Google for your email, they have suggestions for protecting yourself and your data, should this issue occur again (this list of items may be viewed here). However, even if you are working with network security already in place, without using the right tools to protect yourself, you are still at risk. We have three suggestions for what could help you reduce your risk and your exposure to these attacks.

### 1. Decrease Your Risk with Spam Filtering & Anti-Virus Software

To help decrease your risk of running into these email spoofs, be sure to invest in a reliable spam filtering and anti-virus software. Check to see if your email system already has a spam filter and talk with your IT provider to find out if you need to add additional protection.

In addition, anti-virus software is critical to protect your computers and servers if viruses make it on to the network. Be sure that your IT company is keeping your software current and virus definitions updated to dramatically decrease your risk.

## 2. Calm Your Concerns with Advanced Security

When it comes to the IT management for your company, be sure that you have implemented a strong solution for security. A traditional firewall may no longer be enough to protect you. Utilizing a firewall that includes security services such as gateway anti-virus, intrusion prevention services, content filtering, and more is key to protecting your network. Mode5 utilizes an *Advanced Security* service, which wraps all these features and more into one package. Taking these security measures will decrease your risk of hacking and keep your mind at ease.

## 3. Decrease Your Risk by Educating Your Users

Ultimately, these types of attacks can be prevented with several steps that you can take to protect your data and your business. Be sure to educate your staff on how to prevent email scams by instructing them to: be cautious of strange email addresses, read through the messages carefully, keep an eye out for poor grammar and generic greetings, stay away from clicking on suspicious email banners, avoid opening attached documents from unknown senders, and to take caution when clicking on email links.

These spammers and scammers will not stop working hard at trying to hack you and invade your networks. Taking these steps will help decrease your risk of these infections, so be sure you’re working with an IT company that is keeping you protected.

**Questions?** Please feel free to reach out to us with any comments or questions at 757-628-8324. You may also follow us on social media for updates on seminars, lunch & learns, webinars, and more.