Let's Go Phishing!

Insights
3.03.17

Emails, lots and lots of emails, filling our inboxes. Even with the best security and filters, it seems that hackers are simply building better mousetraps. The bigger problem, however, is the trusting nature of individuals who open emails that they shouldn't. Phishing emails appear to come from a trusted source; such as a supervisor, client or government agency.

During the early part of 2016, tax time, more than 40 companies were hit with a phishing scheme designed to collect W-2 information for company employees. BEC (Business Email Compromise / Correspondence) can be used as a form of Spear Phishing to obtain, for example, tax information in order to submit fraudulent tax returns.

Seeing a 400 percent increase in phishing scams in 2016, on February 1, 2017, the IRS warned tax payers of fake emails and websites designed to steal personal information. "The IRS has already seen email schemes in recent weeks targeting tax professionals, payroll professionals, human resources personnel, schools as well as average taxpayers."

The IRS reminds tax payers: "The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information. In addition, IRS does not threaten taxpayers with lawsuits, imprisonment or other enforcement action. Being able to recognize these telltale signs of a phishing or tax scam could save you from becoming a victim."

Even worse, some phishing emails include malware. It goes without saying that the damage a virus can do to a company's computer system can be devastating. What can a business do to ensure protection from phishing schemes sent to unsuspecting employees? Assuming that the company already has in place sufficient data security safeguards (credentialing, firewalls, spam filters, etc.) employees need to be empowered with information to protect themselves and the company.

First, discourage use of company email accounts for personal use, such as online banking, credit cards and tax preparation services. Second, notify employees to be on the lookout for emails requesting personal and/or financial information for the company or a group of employees that appear to come from a supervisor. Employees should be directed to verbally follow up on such requests with the supervisor, and any phishing emails should be reported to the IT department. The same is true of employees who may hold personal and/or financial information for a client or client's employees. Confirm any requests with the client directly before simply responding to an email.

Third, notify employees that requests from government agencies for personal and/or financial information for company employees or clients must go through a designated department or member of management. Finally, remind employees not to open emails that come from a sender they do not know, are unsolicited, ask for their login credentials, include imbedded downloads or simply look suspicious.

Related People

Michelle I. Anderson
Partner
504.529.3839
Email