



NONPROFIT

Nonprofits Beware: Pfishing Trips

12.20.17 | Linda J. Rosenthal, JD



“Do you have a phish story you would like to share?”

That’s the question the folks at the [Anti-Phishing Working Group \(APWG\)](#) want to know. The APWG is a worldwide coalition of representatives from industry, government, law enforcement, and NGOs. Its purpose is to bring together the “global response to cybercrime.”

In November 2016, we posted about the urgency of this subject in [Nonprofits and Cybersecurity: Make it a Priority](#). “Hacking is big news these days.” A year later, we now know how much this was an almost naive understatement. Barely a week goes by without news of yet another major cybercrime; allegations of major internet intrusions dominate not only business but also political coverage in the media.

Pfishing: The Danger

Just last month, in November 2017, we again addressed this topic. “Phishing,” we explained in [Key Cybersecurity Threats for Nonprofits](#), is now one of the three most common cyber threats.

Phishing – the word – is not new, although only recently has it started popping up in mainstream media stories and worried conversations at the office coffee bar. Almost two decades ago, in 1996, hackers were surreptitiously grabbing accounts and passwords of America Online users. Using email “lures,” they set out hooks to “fish” for valuable data from the “sea” of Internet users. The analogy to the sport of angling was obvious enough that the term “pfishing” emerged.

How does pfishing work? It begins with a fraudulent email “designed to entice” the one who receives it to open it, click on an attachment, or respond to it. These sophisticated cyber intrusions



are themselves bad enough without an extra element of danger and damage: They are set up to go undetected for weeks or months.

Worse yet, phishing has now routinely become weaponized – with ransomware. Simply put, a successful phishing intrusion is followed up by a ransom demand: Pay us lots of money to go away, or we'll continue to hold you and your valuable information hostage. The ransomware element – like phishing – is not a new phenomenon.

“In 2016, ... phishing went mainstream. Fast-forward just six months into 2017, and it already appears that phishing will have an even greater impact on the world by year's end,” warns cybersecurity firm Ironscales six months ago. “Ransomware attacks rise 250 percent in 2017, hitting U.S. hardest,” blares a Newsweek headline in late May 2017. Many of these are mobile ransomware attacks – called “smishing” – delivered via SMS text phishing.

Security experts describe ransomware “as the ‘go-to method of attack’ for cybercriminals and the ‘epidemic of our time.’”

Form W-2 Phishing: IRS Warns

While cyber attacks of all kinds are dangerous threats, the Internal Revenue Service issued a specific warning early in 2017 about a practice that targets certain entities including nonprofits: the Form W-2 Spear-phishing Scam. The human resources departments of school districts, tribal governments, and certain tax-exempt organizations have informed authorities they are receiving “bogus emails” that request employee W-2 tax information. (In 2016, similar scams were reported by for-profit firms.)

The 2017 IRS warning bulletin includes common examples that had appeared during the 2016 tax season. For example, a false email under the name of an existing supervisory employee would be sent to a person in the organization with access to financial and worker data, with language like: “Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review.” Similarly, a scam message might read: “Can you send me the updated list of employees with full details (Name, Social Security Number, Date of Birth, Home Address, Salary).” Or a trusting worker might receive and act on a direction like this: “I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me ASAP.”

Because nonprofits are required by law to make some of their information available to the public, they are particularly vulnerable to phishing scams like these. The hackers already have considerable preliminary information available from organization websites; cybercriminals can copy logos and signatures, for instance, that help make the phishing emails look authentic. Form 990s and annual reports posted online or that are accessible otherwise give hackers names, titles, and salaries of key personnel.

Conclusion

Cybercrime is an enormous public threat and grows more dangerous and sophisticated each day. All businesses, governments, organizations, and individuals must learn about it, and take precautions



commensurate with the enormous danger.

Nonprofits must take heed of this IRS notice and other specific warnings. This is not the concern of only the IT department or just a few executives or other people. Nonprofit boards must take the initiative – immediately – to educate themselves about this topic even though it is complex and highly technical. They must take necessary steps to minimize existing and foreseeable risks. We'll return to this topic again in future posts; there's no possibility – unfortunately – that it will fade away from any list of top global concerns.