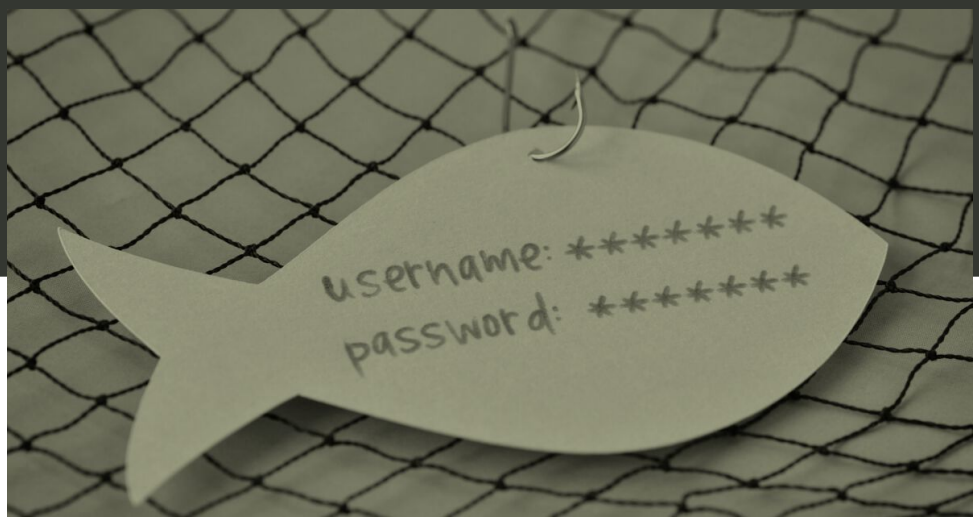
FPLG
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

Another Pfishing Tale

01.07.19 | Linda J. Rosenthal, JD



Headquartered in suburban Baltimore, the Harry and Jeanette Weinberg Foundation is one of the nation's largest private charitable foundations with annual grants topping $100 million each year. The primary recipients are nonprofit service providers to low-income and vulnerable people in the United States and Israel.

A side project is the Israel Mission program, in which community and government leaders, mainly from Maryland, are taken to Israel for an "intense educational orientation" including the opportunity to meet Israeli leaders and community representatives. Out of this successful endeavor came the Alumni Scholars Program, now a group of some 600 past participants in the Israel Mission. There are now annual educational events as well as an alumni directory and reunion dinners.

In early June 2018, one of these Alumni Scholars opened an email that appeared to be from the Foundation but didn't look quite … kosher. He called Craig Demchak, the Foundation's director of marketing and communications, who understood right away what happened. The Foundation was the victim of a cybersecurity breach into its computers and databases; the scheme was in the form of a now-all-too-common scheme, a "pfishing email" intrusion.

Mr. Demchak immediately took action including posting an alert on the Foundation's website to inform supporters about the phony email scheme. Part of this warning including the following language:

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. In this case, the perpetrator has used source emails which appear to be from the Weinberg Foundation, but which are not. Phishing is typically carried out by means including email spoofing, often directing users to enter personal information at a fake website (or a donation portal—even one that is legitimate, in this case Paypal).

Readers were told to ignore any such phony email solicitations. The matter continues to be under investigation.

Pfishing Email Schemes

The pfishing email in The Weinberg Foundation case indeed "appears to be of the typical pfishing variety."

These emails generally "seek to obtain information by posing as a familiar and trusted entity." The cyber breach can go on for a while without being discovered because the named sender has not in fact sent the email, so is unaware of its existence until and unless someone receiving one of the emails gets suspicious and reports it. Without the quick action of the Scholar who alerted the Foundation official of his suspicions, this cyber intrusion may have continued without detection, all the while causing significant damage.

In 2017, we highlighted this insidious practice in *Key Cybersecurity Threats for Nonprofits* and *Nonprofits Beware: Pfishing Trips* which had been identified as one of the three most common cyber threats, although its origin dates back to the earliest days of the internet in the 1990s.

"'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.'" Why the play on the word "fishing"?: "(u)sing email 'lures,' [the earliest hackers] 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."

Widespread Pfishing Vulnerability

"In 2016, … phishing went mainstream"; by 2017, it had escalated dramatically. Worse still, pfishing is often weaponized by adding a "ransomware" element. The hackers make the intrusion, let it cause some damage, and then demand a ransom amount to remove it. Ransomware is now to "go-to-method of attack"; the "epidemic of our time."

We wrote in *Nonprofits Beware: Pfishing Trips* that early in 2017, the Internal Revenue Service issued a specific warning about a practice that targets certain entities including nonprofits: the Form W-2 Spear-phishing Scam. This notice includes common examples that had appeared during the 2016 tax season and which were brought to the government's attention by groups that had been victimized.

One such example is a phony email under the name of an existing supervisor sent to the person in an organization with access to financial data or worker information; the language would be something 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."

Nonprofits are particularly appealing targets for hackers because (1) some

groups are required by law to make certain information available to the public, and (2) substantial information is available from organization websites (including logos and signatures that can be copied) and Form 990s and annual reports.

Conclusion

Cybersecurity must now be at or near the top of each and every nonprofit's risk-management strategy. It's not a matter that can be punted over to one person or a consultant; it must be addressed head-on by the board of directors. Necessary steps include become fully informed about the nature and extent of various threats, available precautionary steps and insurance coverage, and the organization's responsibilities under law.

Many states, including California, have laws on the books requiring immediate action by any hacked organization, especially where outsiders' data have been compromised. California has updated its data security breach notification laws, from time to time, including amendments effective January 1, 2016 to California Civil Code sections 1798.29 and 1798.82.

At the end of June 2018, the California legislature passed, and Governor Jerry Brown signed into law, a sweeping new data privacy law similar to – although not quite as tough as the European Union's GDPR that went into effect on May 25, 2018. It appears that California's new law may exempt nonprofits, but the GDPR does not have such a blanket exemption and does, indeed, affect certain larger nonprofits in the United States.