



The Merits OF Phishing Your Own Employees

by [Steve Brown](#) Topics: [cyber risk](#), [cybersecurity](#), [risk management](#)

Summary: Phishing is still a big problem. One of the best ways to educate people within your bank about the risks is to actually phish them on an ongoing basis.

Fishing is one of the most popular outdoor recreational activities in the US, but you may not know these interesting facts from The Fish Site we uncovered: catfish have 27,000 taste buds vs. 9,000 for humans; lobsters have longer life spans than cats or dogs and live 20Ys; and the typical fish brain is about 1/15 the mass of a similarly sized bird or mammal. Meanwhile, Statista reports that in 2017, more than 49mm Americans participated in freshwater, saltwater and fly fishing.

Many people like to fish it seems, but phishing of another variety is not so popular in banking circles. Despite the increasing complexity of the measures that cybercriminals use, phishing emails still remain one of their most effective tactics.

While the majority of spam and phishing emails people get remain easy enough to identify (simple misspellings, poor English, poor structure), it only takes one person to click to cause a cascading nightmare.

Sadly, not all phishing emails are so easy to spot, especially with the increasing use of legitimate contact software and apps sending email updates. Adding to the email chaos is the fact that cybercriminals have stepped up their game by taking the time to learn about specific individuals or groups by using more targeted efforts. This ups the ante and the risk.

One of the best ways to educate people within your bank about the risks is to actually phish them on an ongoing basis. To do this, start with your Risk and IT departments and send "test" phishing emails to employees. This will give you a good idea what could happen if a real phishing email came in, with response rates, and offer the opportunity to increase awareness and training.

It is also important to teach employees that phishing risks are not just limited to work e-mail accounts, but can also come from social media accounts and personal emails too. This is particularly true when people use the same or similar passwords for both personal and work accounts, or if such accounts are linked to work accounts.

According to a CPA and cybersecurity advisory firm, 90% of the world's cyber attacks begin with phishing emails. Among the types of phishing messages that employees most commonly click on are: messages from human resources; voicemail notifications; notifications from regulatory agencies, vendors or associations; and social media messages.

Another area that may help is to train your staff what not to put in their regular emails. Providing some internal guidance here could reduce the anxiety about the legitimate emails sent in the scope of regular business activities, while learning about the pitfalls of the illegitimate kind.

Some tips here include: tell people ahead of time that you will send an email; if possible, put the complete message in the email vs an attachment or link to avoid any unnecessary concern.

Of course, cybersecurity and employee training require constant updates and review, especially with new employees, but that isn't where it ends. It is also critical to remind even tech-savvy, seasoned employees too, because no one is immune. The attacks are relentless and it only takes one click to cause a significant and possibly expensive issue for the bank.

ECONOMY & RATES

Rates As Of: 03/19/2019 04:38PM (PDT)

Treasury	Yields	MTD Chg	YTD Chg
3M	2.44	0.01	0.09
6M	2.51	0.01	0.03
1Y	2.49	-0.04	-0.10
2Y	2.47	-0.05	-0.02
5Y	2.43	-0.09	-0.09
10Y	2.61	-0.10	-0.07
30Y	3.02	-0.06	0.01
FF Market	FF Target	Fed Disc	
2.40	2.50	3.00	
SOFR	Prime	Unemp	
2.41	5.50	3.80	

[More Market Rates](#)

BANK NEWS

Malware Alert

A decade-old [banking malware known as Ursnif is making a comeback](#) after its source code was "leaked" to global cyberthieves (that tweaked it and made it more deadly). Ursnif coupled with the banking Trojan, Bebloh, pulls not only data, but also scrapes emails and browsers for a plethora of sensitive info. It begins with phishing emails, then downloads through the guise of an invoice or other document, ensures it is not in a sandbox, then runs right before shutdown to minimize detection.

Employee Development

[A survey by the Society for Human Resource Management](#) (SHRM) finds 86% of respondents say their companies offer professional development opportunities for employees and 45% offer cross training not directly related to an employee's job to help improve skills.

AML Pressure Continues

The OCC instructed MUFG Bank to beef up their AML controls, as the regulator found various branches "failed to file reports on suspicious customer activity in a timely manner and that there were 'systemic deficiencies' in how the branches monitored high-risk transactions and correspondent accounts for foreign financial institutions." Also, Capital One indicated in its annual filing there may be "additional government fines or penalties" due to AML program issues. The bank received a consent order related to its BSA/AML compliance back in July 2015 and paid a civil penalty of \$100mm last October.

WHITE PAPER: TRANSITIONING TO SOFR

Bankers have heard that SOFR will replace LIBOR as a benchmark in 2021. But, what is involved in this transition? To learn more about the impact and how your bank can plan for it, download our white paper, "[Moving from LIBOR to SOFR: Smoothing the Transition for your Financial Institution](#)" now.

Copyright 2018 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.