Helping Customers Avoid the Phishing Net

by Steve Brown

Between 1959 and 1976 it is estimated that more than 6mm dolphin deaths occurred due to tuna fishing in regions of the eastern tropical Pacific Ocean. Since that time, mortality numbers have fallen significantly thanks in part to new laws designed to protect dolphins and a concerted effort by various groups to protect these aquatic mammals. We like to eat tuna, but we also like dolphins (one of the smartest mammals on earth), so we think balancing fishing activities makes sense.

Like the nets that trap dolphins, despite the financial services industry's best efforts to eradicate its own sort of phishing, there are still many fraudsters lurking where they aren't supposed to be. Just the other day we received an email from one such phony, warning us about some allegedly fraudulent activity on an account of ours. We did not verify any of our personal information, of course, but the email got us wondering how banks can remain vigilant when it only takes one click to release danger. How do you warn and protect your customers against the ongoing danger of Internet fraud with millions of phish swimming around trying to get caught?

The latest data around phishing suggests that e-criminals aren't giving up and continue to look for new opportunities, and banks certainly aren't immune and remain a prime target.

In fact, according to the Global Phishing Survey for 1H 2013, there were 720 unique targeted institutions during the period, up significantly from the 611 found in 2H 2012. Not surprisingly, PayPal was most often targeted, while banks accounted for 40% of the attacks during the period. Meanwhile, the top 80 targets were attacked 100 or more times each in the period.

During the holidays, that data also shows that instances of fraud tend to accelerate, so now's a good time to reach out to customers to remind them to protect themselves. Checking online statements more frequently and holding tight to personal information may seem like no-brainers, but there wouldn't be fraud if there weren't ample targets to be had.

Bankers may also want to tell customers what to do if they receive emails that purport to be from the bank. Many banks have links on their websites to allow customers to report these fraudulent attempts. The question is: how easy is it for customers to find these links to report problems or forward suspicious emails? Are they right on your homepage in plain site or do they have to click around trying to figure out where to go? Have an email dedicated to abuse reports, so you can take the necessary measures to protect customers and your bank from harm.

If you haven't done so in awhile, it's also worth reminding customers that you'll never, under any circumstances, send them an email or a text or call them asking them for their account numbers or passwords. Remind your customer contact personnel to make sure customers know they should never give sensitive information over the phone or in a text or email to anyone, ever.

Since the "dolphin-safe" movement came about there have been many strides to protect these amazingly happy and smart sea creatures from over fishing. Banks, too, need to continually remind customers and staff alike to avoid their own sort of phishing lures as they travel the sea of information on the internet and through email. It makes good business sense and this time of year it

is a nice reminder for a bank to share with its customer base to be sure they start 2014 happy, healthy and safe.

BANK NEWS

Mobile Competition

Wells Fargo said it will link its Visa credit card to the Isis Mobile Wallet (joint venture between AT&T, Verizon and T-Mobile), allowing customers to load cards into the mobile wallet application to make purchases. Wells follows JPMorgan and American Express who previously announced they would join Isis.

Cutting Back

The Federal Housing Finance Agency (FHFA) is seeking comment on a plan that would gradually reduce the maximum size of loans FNMA and FHLMC could guarantee. The plan lowers the loan limit from $417,000 to $400,000 nationwide and from $625,500 to $600,000 in high cost areas starting after Oct 1 2014.

Security Risk

NSS Labs has released a report that finds commonly used one time pass codes sent by banks to customers through text short message service (SMS) are increasingly ineffective and have been "thoroughly compromised." The report urged banks to enhance security to include combinations of "hardened browsers, certificate based identification, unique install keys, in-app encryption, geolocation and device fingerprinting" to better secure transactions.

Mobile

A Harris Poll finds the main reasons some people are not using a smartphone to process payments is that they are already happy with cash and cards (53%) or have security concerns (53%).

Customers

A TD Bank survey of US consumers finds only 12% have switched banking providers in the last 2Ys. Meanwhile, the same survey found the top reasons people closed accounts were because of basic account fees (21%), they moved to another state (11%), customer service issues (10%), brand image (7%), extra or added fees (7%), inconvenient branch location (5%), minimum balance requirements (4%) and errors (4%).

Settlement

A federal judge has approved a settlement between Visa, MasterCard & major credit card issuing banks for $6.05B related to a lawsuit by retailers around interchange fees.

Projection

Wells Fargo projects 2.4% GDP in 2014.

Copyright 2021 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.