Phishing the Social Currents

By Robert Capps, vice president of Business Development, NuData Security

Fishing isn't what it used to be. These days, it's all about gadgets and pontoon boats and carbon fiber rods, but essentially it's still the same ol' thing. Drop a line in and try to get a bite. The same can be said for the cyber-phishing world, but not only has the gear changed, so has the lake.

Social Phishing – Not What You Think

Not to overuse our fishing metaphor, but it must be a fraudster's dream to have such abundant and lucrative digital streams in which to sink their lines. While consumers (the fish) merrily go about posting away in social streams, the phishers are ready to hook them. It's true that online users are increasingly aware of suspicious of email and are awakening to the rising vulnerabilities associated with mobile devices. Social media, however, is largely an uncharted territory that users' vigilance hasn't yet mapped.

The most recent example of this is when bank customers were conned in a devilish social media scheme to gave up the keys to their bank accounts by a brazen impersonation of an online bank during a system outage. Fraudsters, posing as customer care agents representing the bank, targeted customers who complained about the outage on Twitter with a phishing attack that had these unhappy, and unfortunate, customers coughing up the keys to the kingdom in a click

or two. Particularly troubling about this type of attack vector is the fact that in many cases, unlike in credit card theft, customers are often held directly responsible for any losses to their account following the disclosure their credentials to a third party.

While phishing schemes that are used to steal user login credentials and personally identifiable information (PII) aren't particularly new, using social media to impersonate the customer care function at an online institution during a system outage is a unique twist on an old scheme. This sophisticated scheme would not immediately raise an alarm for saavy users that may be at an elevated level of concern over cybercrime and identity theft.

The idea that there may be hooks in the social waters might not have occurred to users who've enjoyed the relatively playful and carefree aspect of the variety of social media apps available. This lack of awareness within social media can certainly create an opportunity for these scammers to leverage and perpetrate trust-based crime.

Over the last few years, there has been steady growth in the frequency, maturity, and complexity of social scams and attacks that use integrated approaches involving social apps along with email. In 2014, Symantec reported complex social engineering activity on Twitter with weight-loss scams and celebrity impersonation accounts. Social engineering scams have evolved to leverage other breaches, as in the 2015 Ashley Madison hack where scammers used social engineering to blackmail victims. Instagram has been hit with a variety of phishing scams looking for login credentials, LinkedIn warns users to be "incredibly careful about invitations," and we have the sense that attacking us in our social channels has just begun.

Social media scams can involve phishing, spear-phishing, ransomware and malware, and are almost always financially motivated. What gets lost in all this is that at the root of these scams hackers are collecting the user's valuable data with the intent to perpetrate future account-based attacks and make money. Fraudsters will do that by selling this data on the Dark Web, where other criminals will buy it and use it to take over a legitimate user's account to drain the account outright or perpetrate fraudulent transactions. If the data is sufficiently comprehensive, it can be used for new account fraud, sometimes called application and loan fraud. Under this scenario, the fraudster impersonates a legitimate person and will open an account with the intention of not paying back the institution. There are several variations on this theme such as letting the new account sit dormant to establish credibility over time.

And, the numbers aren't encouraging. In 2015 Auriemma Group found that account takeover fraud involving debit cards was up 280%. NuData's threat intelligence at the end of 2016 found that 60% of new account creations were fraudulent compared to 39% in 2015. In an ecosystem where banks are increasingly under regulatory pressure to tighten cybersecurity, calls are growing louder for banks to become responsible for account takeover losses. Financial institutions are also feeling the effects of the EMVconversion that has had the effect of forcing criminals to change their attack methods from credit cards to online channels and are deploying increasingly creative attack vectors.

The Same Old Warnings

There is no doubt that customers need to be careful online. By now we're familiar with the data that shows 55% of people use the same password everywhere. Symantec notes that more than a third of users who share passwords in the US have also shared the password to their online banking account. Customers have been warned repeatedly. Greater awareness and diligence would be helpful, but it's clear that the scale of the problem can't be reduced by simple warnings like "never use the same password" and "don't open emails from people you don't trust". Socially engineered scams are becoming so sophisticated that even the savviest of users can be fooled. LinkedIn encourages people to be careful of who they follow on social media, and it can be the case that many social media profiles are not actual people but bots designed to deceive and lure users to divulge personal data.

A Way Out for Institutions

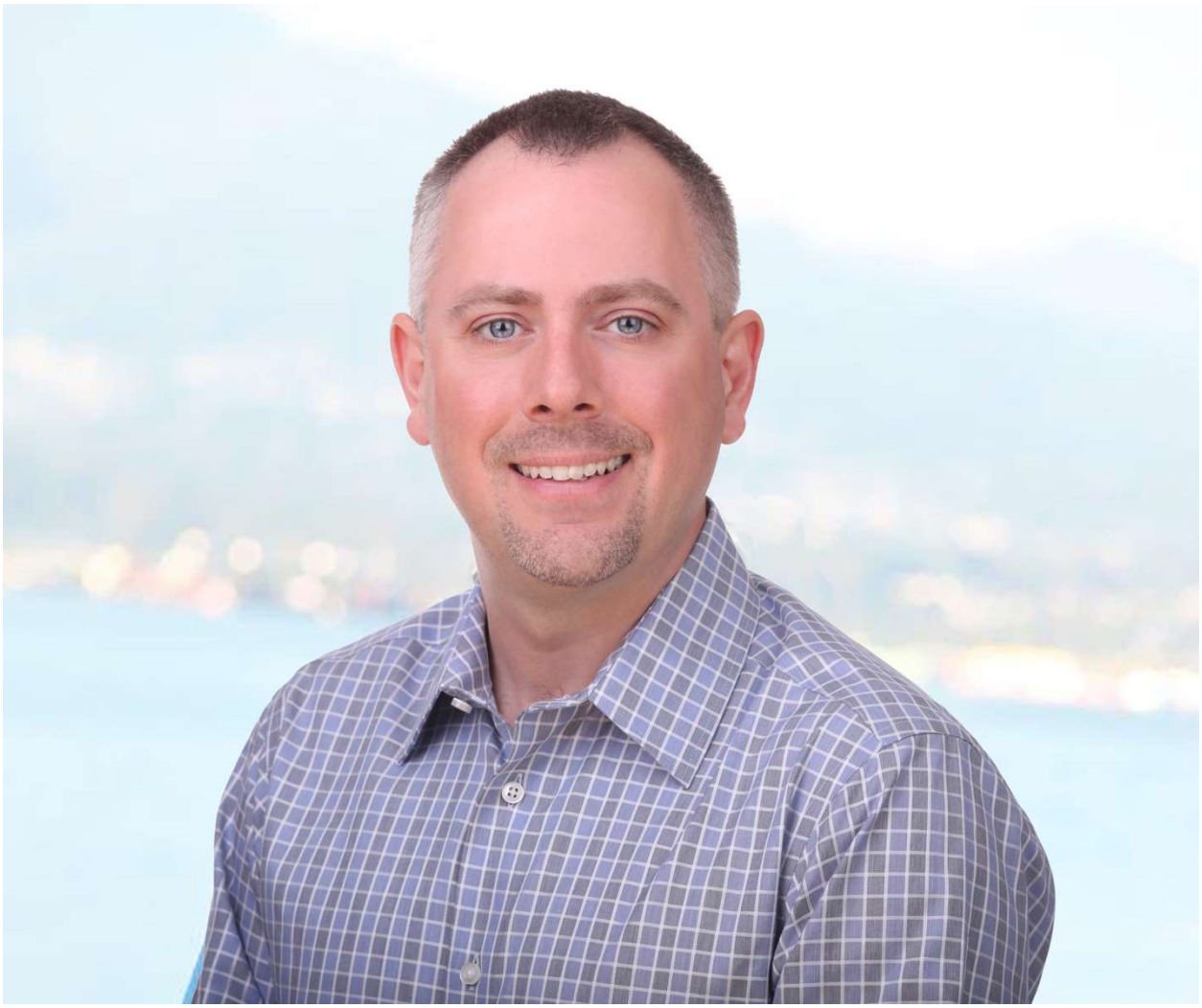
With username and password being two of the most sought after data points in the criminal underground, most online organizations are looking to adopt verification methods that don't just rely on static data points such as user credential. Instead, many institutions are moving to methods that use multiple factors. As multi-factor authentication becomes the new standard in user verification, it is blatantly clear that if fraudsters are to be stopped, financial organizations will need as much information as possible about the real users to combat the proliferation of stolen Personal Identification Information (PII) online. The best way to get more data about users and understand how they act is to analyze the behavioral data they are already offering.

Banks and credit unions need to take a more nuanced approach to authentication, and evaluate as much contextual information about customer interactions as possible to determine if it truly is the right user presenting themselves. Passive biometrics and behavioral analytics technology can distinguish good from bad users even when new devices and correct stolen credentials are used because they rely on a different set of keys – the good customer's behavior. These solutions seem to be a perfect fit to restore customer trust in online channels while adding real security to the login process. A significant benefit of passive biometrics is that they reduce customer friction because that they do not require customers to take additional steps to complete a transaction, and require no enrollment, unlike physical biometrics. Also, systems that can passively collect and analyze live customer data in real-time will have distinct advantages over systems that result in customer loss due to delay and friction.

Working and playing the social streams and lakes is likely to become more dangerous as the crooks grow more adept at exploiting these channels. While social apps and tools can enhance customer experiences by enabling them to communicate and collaborate with each other, there is an unwelcome lesson that these zones are also fraught with danger. It was inevitable that fraudsters would migrate to our social streams and lakes and try to harvest consumer data. Financial organizations can offensively cut their lines and dull their hooks. Organizations that implement advanced multi-factor identity verification systems gain the ability to identify good from bad customers, and can even provide VIP user experiences for those users that have deserved a premium. In this way, the bad guys can be thwarted while good customers enjoy the convenience of enhanced online interactions with their favorite credit unions without the fear

of identity theft or having their accounts drained.

_____



About the author:
Robert Capps is the vice president of Business Development for NuData Security. He is a recognized technologist, thought leader and advisor with more than 20 years of experience in the design, management and protection of complex information systems – leveraging people, process and technology to counter cyber risks.