nxg|strategies℠ Newsletter

10/24/2018

NXG Strategies: Fraud Education Series: Vishing

Authored by Sally King, Co-Founder and Managing Director NXG Strategies

Sophisticated predators are both online and offline, and are preying on your customers daily. Below is the first in a series of articles you can use to help your customers understand more about the latest scams and techniques criminals are using, and how they can better protect their identity. To learn more about our solutions for identity detection and recovery, join us for a free webinar.

Two Minutes and a Phone Call Can Turn Into Identity Theft

There are so many things you can do in under two minutes - brush and floss your teeth, make a delicious cheese quesadilla, walk 200 steps, or become a victim of identity theft! These days, identity theft doesn't just come from cyber criminals hacking multimillion-dollar organizations to steal data, it's also criminals gathering data from a simple two-minute phone conversation that could put you at risk for identity theft.

How can a phone call put me at risk for identity theft?

Criminals can use your phone number along with a natural inclination to trust people to deceive and manipulate you into divulging confidential personal information, which is called "Social Engineering". Skilled telephone operatives will call unsuspecting consumers, often using the guise of a familiar institution or authority with an urgent problem needing resolution.

Through carefully crafted dialogue, sprinkled with enough accurate information about you to gain your trust, they may ask for your account numbers, passwords or PINs, credit card security code, and/or social security number. The clever way these crafty criminals pose the questions can fool even the most careful callees. With the ill-gotten information, the criminals can open accounts in your name, gain access to existing accounts, sign up for medical or government benefits and perform other types of identity theft. When criminals target an entire class of consumers for these telephone schemes it is referred to as "Vishing", which is a voice-related version of online Phishing, another common form of Social Engineering.

Real-life Scenario #1: Hold for an agent, please.

Jay received an automated voice call asking him to stay on the line for an urgent message from the Internal Revenue Service. In a stern warning, the automated recording stated that it is a federal law to deceive the IRS and Jay must verify his identity before talking with an IRS agent. One by one, the recording prompted Jay for more information, including his full name, address, birthday, and Social Security number. Jay provided all the requested information, anxiously awaiting the next step to understand why the IRS is trying to reach him. The recording indicated his identity had been verified. The automated voice then stated that "all agents are busy" and someone will call him back.

In reality everyone who gives up their personal information gets the same response. The criminals have what they want. With a name, address, birthdate and Social Security number a criminal can establish fraudulent credit accounts, apply for government benefits and otherwise wreak havoc on Jay's life. This same approach may use the name of a bank or credit

card company and ask for account numbers, PIN's and even usernames and passwords. The idea is to incite fear and urgency and intimidate by using an institution of authority.

Real-life Scenario #2: Local numbers are okay, right?

Bill received an automated voice call from a company claiming to be "Credit Services" and offering to give him lower interest rates. "This is your third and final notice of this offer" was added at the end of the recording to make it sound more urgent. Bill waited on the line as instructed and a very warm, personable women named Jenny got on the line. Jenny stated she had an offer for people living in Bill's local area as a state-sponsored effort to help residents lower their credit card debt. Bill noticed the caller ID looked like a local number so this made him feel more confident the call was genuine. In reality criminals can spoof the caller ID to make it look like any number they want. Jenny went on tell Bill she had several questions to see if he qualified for the special program. She asked Bill how much credit card debt he had and as Bill recounted his card debt Jenny would circle back occasionally to "verify" the information, asking "so you said you have $5,000 outstanding on one of your cards, which one was that?" Or, "I can verify your balance for you I just need your Social Security Number (or card number and three-digit CVV code).

This is an effort to get Bill to disclose the names of his banks and card issuers and his personal information. Once Jenny had successfully obtained enough information she ended the call by telling Bill more information would be coming in the mail to validate his eligibility. This last ploy is an effort to delay the discovery of the fraud to allow the criminals time to either sell Bill's personal information on the dark web or to commit fraudulent transactions themselves.

Real-life Scenario #3: The Fraud Department called, and they need your card back.

Early one morning, Jen received a call from a representative of her bank telling her the bank had blocked two phony credit card charges from out of state and needed her to confirm her card was not lost. The caller identified himself as a Vice President of Fraud Recovery and recited the last four digits of Jen's card number, asking her to verify this card was still in her possession. Jen confirmed. The caller asked Jen to verify her correct address, which he read to her. Telling Jen this incident is part of a wider investigation into fraud affecting customers of the bank, the caller said he would arrange a courier from UPS to come to her home to pick up the card that was used fraudulently, which would aid in the investigation and speed up the process of getting a new card to her. While it seemed odd to Jen the bank would need the cancelled card, the man on the phone was so convincing. When the courier arrived she was careful to note he was driving a UPS truck and had UPS credentials; feeling better about the situation, she inserted her card into the pre-paid shipping envelope and away it went. After a few days Jen decided to call her bank to find out when her new card would arrive only to find the Fraud Department had not reached out to her and there were several purchases made with her card amounting to thousands of dollars.

Part of the reason this scam is successful is the criminal is using a legitimate courier service. This same scam may use double-talk to collect the full card number, CVV code and PIN information over the phone rather than using a courier service.

It is very easy to fall prey to these schemes, no matter your age, your propensity for privacy, or your knowledge of security.

How can I protect myself from Vishing?

- DO NOT give out your personal information in response to an unsolicited phone call. Instead, tell the caller you will hang up and call back to the number listed on the company website.

- Be wary of offers from a company or person you do not know, prize announcements, or promises of unrealistic returns for your money.
- Don’t allow callers to pressure you to make decisions to give the caller what they want, which may include personal information, information about your organization.
- Don’t change your behavior because a caller uses threats of fines or penalties, and hang up immediately if a caller uses obscene or abusive language.
- If a call has you worried and you want to call them back, don’t call the number offered to you by the caller. Call the number on the company’s website, back of your card, or other valid contact references like a bill.