Bank of Botetourt

September 2022

Smishing Attacks in 2022

2022 didn't bring a decrease in the occurrence of cyber-criminal attacks, unfortunately. Quite the opposite in fact. The latest Quarterly Threat Trends & Intelligence Report from Agari and PhishLabs shows that Vishing (voice phishing) cases increased by almost 550% between Q1 2021 and Q1 2022. Smishing (attacks via text messages), increased by over 700% in the first two quarters of 2021.

What's worse, far too many people still can't recognize when a mail, call, or text message is coming from a fraudster rather than a genuine company. Especially since the criminals know just what to say to get people to act as they want.

So what can you do to protect yourself, your employees, and your business from criminals? Learn how Smishing works so you can spot the signs that your team is under attack. And what better way to learn than by looking at some real-life examples of smishing attacks? Let's get to it, then.

What Is Smishing?

Smishing is a type of phishing attack, except that criminals use text messages instead of emails. The scammer sends an SMS message that appears to be from a trustworthy company.

Once opened, the recipient might read that something terrible is about to happen to their account. For example, their credit card is about to be blocked. Or the opposite - a message congratulating the recipient for being a sweepstakes winner or claiming that a gift is on the way to thank them for being a loyal client.

Each such message will also have a link included, clicking on which is supposedly

Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

Bonsack

Buchanan

Care Center

Cave Spring

Daleville

Eagle Rock

Fairfield

LakeWatch

Lexington

Natural Bridge

Peters Creek

Salem

Troutville

www.bankofbotetourt.com
www.facebook.com/botetourt
(540) 591-5000

necessary to "verify the suspicious charges on your account" or to receive the gift. Clicking on the link actually redirects to a website with a "verification" form asking for the recipient's name, address, social security or ID number, and credit card details, for example.

Upon submission, all of this information will be passed on to the criminals. The website might also download malicious software onto the user's mobile, tracking everything that they do on that device afterward.

According to EarthWeb research, during one week alone in April this year, criminals sent 2,649,564,381 smishing messages. Why? Email spam filters keep getting better at recognizing potential phishing emails and marking them accordingly. More importantly, internet users are also getting more suspicious about clicking on any links included in such messages.

Mobile service providers, on the other hand, are still working on reliable text message filtering methods. Cybercriminals can be confident for now that their messages will be received. Text messages also have very high open and click-through rates (from 90% to 99%), and the vast majority are opened in the first 15 minutes. So, for a bulk attack, SMS is even more convenient than emails.

This is especially considering that finding a list of phone numbers to which scammers can send fake messages isn't the slightest problem. Besides attacking a company's main database, criminals also regularly use:

- Phone number lists sold online (mainly on the Darknet).
- Lists made by third-party numbers aggregators.
- Contests, lotteries, and sweepstake entries.
- Social media and website crawlers.

Sometimes, criminals can even find legitimate phone numbers in paper bins outside an office, for example, if the company isn't careful enough about destroying their documentation.

What Kinds of Smishing Text Messages Might You Get?

Once the criminals have a list of phone numbers to attack, what do they do next? Craft a story through which they will try to trick the recipient into sharing sensitive data.

For example, the scammer could pose as a bank representative and alert the victim that someone tried to take a loan in their name.

Clicking on a link would apparently confirm or deny the loan application, but first, the recipient needs to share their bank details to "verify" that they are the actual customer.

Another common story is that the victim has won a voucher or gift bag from a well-known brand (either from a sweepstake/lottery or simply as a "thank you for being a loyal customer"). Of course, they need to confirm their details first through a link included in the message.

Basically, if there's any situation that fraudsters can use for an attack, they will. Whether it's offering "free" help with filing tax reports or governmental benefits paperwork or even gathering money supposedly for charities during natural disasters.

Conclusion

Considering how much success criminals have with text message scams, we can only expect that they will keep using such methods even more often. So how to not fall victim to those scams? For emails and SMS, the best way is simply to not click on any links in them before checking if the message really came from a bank or phone provider.

***Source:** Pavel Jirik, BLOG, August 8, 2022*

Beware The Tactics Used For CEO Fraud By BEC Scammers

Business email compromise (a.k.a. CEO fraud) is the highest-grossing type of cybercrime, according to the FBI's IC3 Internet Crime Report 2021. More than a third of all cybercrime losses can be attributed to BEC scams, causing about $2.4 billion in losses to U.S. businesses last year, a 33% increase from 2020 and a tenfold increase from just seven years ago. Between 2013 and 2019, CEO fraud reportedly cost the economy a staggering $26 billion.
How does a BEC attack work?

A BEC scam is a type of highly targeted social engineering attack where scammers impersonate top-tier executives and then instruct their lower-ranking workers to execute a wire transfer or fake invoice, share bank information, switch payroll information, make gift card purchases or disclose sensitive information, such as personally identifiable information, wage and tax statements or financial statements. The list of CEO fraud tactics is long.

BEC scams typically involve a combination of phishing, social engineering and credential stuffing in which attackers conduct extensive reconnaissance about the target, steal identity details of key executives and trick gullible users into carrying out any number of transactions, including transferring money to a scammer's bank account. Users are the last line of defense but the easiest to breach. Tactics and tools leveraged by cybercriminals to carry out CEO fraud include the following.

Email Spoofing
A spoofed email is an email in which the display name of the email is modified to impersonate a high-ranking official; if one takes a closer look, they will realize the sender's email address doesn't match the actual person's corporate address. Some fraudsters go to the extent of employing a lookalike domain that causes visual confusion (for example, "betsbuy.com" instead of "bestbuy.com").

Email Account Compromise
An email account compromise or account takeover is a technique in which attackers hijack a legitimate user's account so that they can impersonate them. Securing access to legitimate accounts is easier than one thinks. Attackers steal credentials by luring users to fake login pages or purchasing passwords on the dark web, where more than 15 billion compromised accounts are available for sale. Some attackers go to the length of setting up email forwarding rules so they can monitor the target's email conversations.

Virtual Conference Impersonation
Earlier this year, the FBI's cyber unit IC3 reported receiving an increased number of complaints involving the use of conference meeting platforms like Zoom by cybercriminals to lure victims into making wire transfers to fraudulent accounts. How this works is that the unsuspecting employee receives a phishing email from the alleged CEO or another C-level executive with instructions to join the conference. The scammer uses a headshot of the CEO as their profile picture, blaming the lack of video on some audio or camera issue. They then instruct the victim to initiate an urgent wire transfer.

Deepfakes
Deepfake is a type of synthetic content that leverages artificial intelligence and machine learning to produce audio, images or video that has been tampered with or fabricated but is seemingly realistic. Social media enthusiasts have been using deepfakes for entertainment value, but hackers have been eyeing them as an opportunity to create impersonations of trusted sources. Last year, fraudsters cloned the voice of a company executive to successfully convince a bank manager to transfer $35 million to the criminal's account. Deepfake technology is maturing so quickly that experts believe advanced deepfakes could become almost undetectable.

How Organizations Can Reduce The Risk Of A BEC Attack
BEC attacks are becoming more sophisticated by the day and often hide attackers in plain sight by blending in with IP ranges that have high reputation scores. Since BEC relies purely on legitimate channels and is highly targeted, it is extremely hard to detect by spam filters and other security technologies.

Educating and training workers to identify a BEC is the first intervention to reduce the risk of a BEC attack. BEC attacks rely on humans to succeed, so it's critical that employees are taught not to trust anything at face value. They must develop a habit of healthy skepticism and report anything they find suspicious. Employees must be taught the importance of password hygiene, and security teams must deploy multifactor authentication (MFA) so that if credentials get compromised, MFA can prevent attackers from unauthorized access to email accounts.

There really isn't a silver bullet to stopping BEC. To effectively combat it, one must use a defense-in-depth approach that includes a combination of technologies, user awareness, policies and procedures.

Source: *Stu Sjouwerman, Founder and CEO of KnowBe4 Inc., May 18, 2022*