.domainSkate

*BRAND PROTECTION DONE RIGHT

CLIENT MEMO: Brand-based "Smishing" Attacks Use Fake Domain Names To Enhance Scams

The phishing techniques long used by cyber-criminals have grown beyond email to now include text, direct messaging (on platforms like Instagram and Facebook), and other channels. Text and direct messaging based cyber-scams have become a huge problem for companies and users alike. Almost everyone has received a text tied to companies like Amazon, Netflix, Walmart, as well as smaller entities like regional banks and businesses.

The rise in text based cyber-scams is partly due to the fact that email is becoming a less effective format. This is a result of safety and anti-spamming measures that providers have implemented, as well as increased public awareness. At the same time, mobile scams are increasing because more people are surfing the web via their phones - as of late 2020 mobile web-traffic accounted for approximately half of the world's web-traffic, and 85% of the cyber-attacks seen on mobile devices now take place via mediums other than email. *See* Verizon 2020 MSI Report.

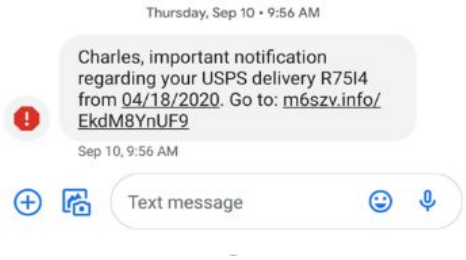
Even more compelling, most people open the text messages they receive (98% according to marketing statistics, with a 45% response rate), while people open roughly 20% of the emails they get (with a 6% response rate). *See* data from EZMarketing.com. This is where "Smishing" comes in.

Smishing is basically the same thing as a regular email based phishing scam, but instead of using email, the scammer sends a text or message using a messaging app and targets the victim's smartphone. By tapping on the link in the smishing message the user will either: (i) unknowingly install malware on the their phone, which can then take and harvest data from the phone for the scammers, or (ii) direct them to a malicious site that will ask for data, personal information, money, and the like.

How Smishing Works:

A smishing attack typically plays out in the following way:

1. A cybercriminal sends an SMS text from a fake number. The content and number make it seem like it came from a legitimate business and may even be tailored by pretending to be from a company or service you actually use (such as your streaming service or bank).



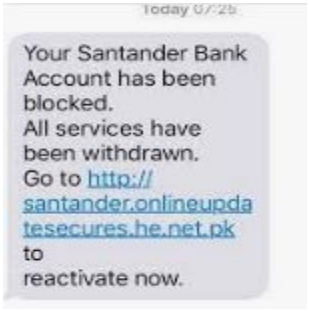
2. The message asks you to respond, by making an offer, or asking you to take care of an issue or problem that requires you to act on the message.

3. If you ignore the message or block it, the scam has been stopped. BUT, if you respond by clicking on the link, you'll be directed to a fake website that will seem like a legitimate business. Here you will be prompted to provide personal information or download

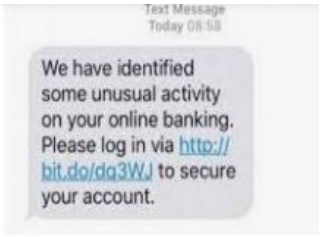
something to your device before you can proceed. If you do this, then the scam has hit its mark and you will either have handed over your personal information to a cybercriminal, or given them access to your device and/or accounts.

Smishing Domain Names - What To Look For:

A crucial part of the smishing grift is the cyber-criminal's use of a fake website and domain

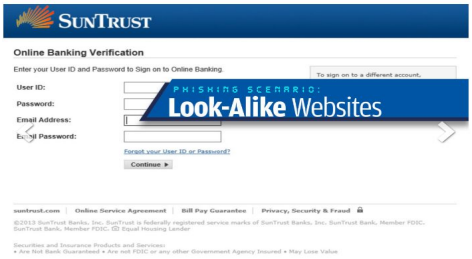


name that jibes with the user's expectation that they will land at a legitimate business website, so that they can feel comfortable handing over sensitive information. While the text may use the actual domain name in the message (like the one above which uses SANTANDER), very often



the actual domain name in the smishing text won't look like the fake domain (see the example above) because text messages typically use URL shorteners for website links that are embedded in the message. Once the user clicks on the link, the domain name and website will likely look

pretty legit. It is easy for any attacker to rip the HTML off a company website, paste it to the fake site, and make it look good. See below:



Steps You Can Take To Protect Your Company/Brand:

From a brand perspective, a targeted smishing campaign can have a devastating effect on consumer trust. Cyber-criminals can send tens of thousands of messages to unsuspecting users and with devastating consequences to personal security. To keep your companies name out of the cyber-crime headlines, here are three (3) steps you can take:

1. Make it clear to your customers/users that you will NEVER ask them to verify account information through text messages, social channels, or email solicitations. You should state this clearly in any/all terms and conditions or user agreements that are public facing, and in direct client messaging/forums that users frequent;
2. Monitor your online presence for fake domain names and websites that could be used as base for smishing attacks - particularly if the site has gone so far as to rip the HTML off your legitimate website to make it look like a branded site. As soon as you see this kind of site, move swiftly to have it taken down or disabled. Further, if there is any identifying information from the attacker - such as an IP Address, Nameserver, or WHOIS admin information, look to see if there is any overlap with other domain names or existing websites; and
3. Deputize your users/customers' as your brand's eyes and ears by letting them notify you about potential smishing scams. This can go a long way to making customers feel like

you take their privacy and security seriously, and that they have a way to communicate problems to your company. This can be an effective first line of defense to prevent damage on a large scale.