What You Need to Know About “Smishing” Scams

DON’T LET THE cute-sounding name fool you: Smishing is when cybercriminals use text messages to lure victims. (The word is a portmanteau of “phishing,” in which victims are lured via email, and “SMS,” the protocol used by most phone text messaging services.) Smishers have found that people are more likely to open a potentially suspicious text message than email message, and that personal devices generally lack the type of security available on corporate PCs.

Here’s how to recognize—and avoid—three types of scams popular with smishers:

1. They try to trick you into revealing account login credentials. Smishers may try to convince you to give up a username/password combo or other confidential info that they can use to log into an online account—paradoxically, by playing on your fears of being hacked. They’ll send a text claiming to be from your bank, warning you about a large transfer, for example, and giving you a link to click on to block this potentially unauthorized access. In reality, the link sends you to a spoofed website that looks like your bank’s and asks for your username and password, and the phone number connects you to the scam artists. Once they’re armed with your credentials, they can log into your bank account.

2. They try to get you to download malware. This is similar to one of the primary goals of phishing, adapted for mobile users and mobile technology. In one recent incident, a smishing scam in the Czech Republic convinced users to download an app purporting to be from that nation’s postal service; in reality, it was a malicious program that could harvest credit card info entered into other apps on the phone.

3. They ask you to send money. This is more the domain of the con artist than the tech wizard, but it’s still a real concern. Smishers will do some work to get you to trust them; in one attack, a woman in Tennessee received texts she thought were from personal friends (the names had probably been harvested from Facebook) telling her about a government grant she qualified for. In reality, this was a classic “advance fee” scam. The victim was told she had to pay a few hundred dollars up front for “taxes” to get the money. Keep in mind that offers that seem too good to be true usually are.

Legitimate messages should contain information proving that the bank already knows who you are, such as the last few digits of your credit card or bank account number. Be suspicious of vague references to “your account” without any details. If a message looks dodgy, log into your account via your browser or app without following any link sent to you in a text.

How to report unwanted texts:

- In your messaging app, look for the option to report junk or spam.
- Report spam or junk in the Messages app.
- Report spam on an Android phone.
- Copy the message and forward it to 7726 (or SPAM).
How to Survive—and Thrive—While Working from Home

As a result of the coronavirus pandemic, employees in many sectors are working from home for the first time. The adjustment can be challenging, to say the least. Below, business and technology journalist Steven J. Vaughan-Nichols, who has been working full time from home for 30 years, shares his strategies for staying sane and productive.

• Get out and walk. Sitting down all day long isn’t good for your health, physical or mental. I walk for half an hour twice a day.

• Keep regular business hours. There are two common time problems with working from home. The first is: “I’m at home, so I can watch TV, I can play World of Warcraft, I can... whoa, what time is it?” The other is: “I’m at work, and must work all the time. I must... whoa, what time is it?” If you work 9 to 5 at the office, try to work 9 to 5 at home.

• Stick to your diet. Snacks are so accessible, and no one is watching! Also, we all tend to eat more when we’re under stress, and boy, are we ever stressed out these days. Try to eat healthy snacks. Your scale (and your work clothes, which you’ll have to get back into eventually) will thank you.

• Dress for work. You may be tempted to wear your jammies or your favorite T-shirt to work. Don’t give in to this unless you habitually work in comfy clothes anyway. If you’ve always worn business attire, sweatpants and flip-flops won’t feel like work to you, so keep wearing at least a modified version of your business clothes to get into the right frame of mind.

• Set up a dedicated area for work. It can be as small as a cordoned-off section of your kitchen table. But scattering work across your home leads to scattered thought.

• Make it clear to your family or roommates that when you’re at work, you’re at work, even when you’re at home. You’re not available—but you’re not inaccessibly locked down either. Set your limits, but still pay attention to the others at home. After all, you talk to people at the office, right?

• Get a comfortable chair. Unless you use a standing desk, you’re going to be spending a lot of time in that chair. It’s worth spending some real money on a good one.

• Use your new home videoconferencing gear and IM software to talk to friends and family. I’m an introvert’s introvert, but I still talk to my people on a regular basis. They help keep me together, and your folks will do the same for you—and vice versa.

• Don’t obsess over the news or check social media every five minutes. Strive not to give in to temptation. It won’t help any, and it will probably add to your stress.

You may never love working at home. It’s great for me, but it’s NOT, in big capital letters, for everyone. Still, if you follow my advice, you’ll get good work done and come out on the other side with your wits still about you.

What Happened in the July Twitter Hack?

ATTACKERS OFTEN IMPERSONATE celebrities on Twitter to post scam messages, usually using fake accounts with few followers. But on July 15, as part of a cryptocurrency scam, the Twitter accounts of Bill Gates, Jeff Bezos, Barack Obama, Joe Biden, Kanye West, Kim Kardashian, Uber, Apple, and even Twitter’s own official support account, among others, posted messages asking for donations via bitcoin, a cryptocurrency popular with scammers because lost funds can almost never be recovered.

Because these rogue messages were posted from verified accounts, the scam appeared more credible and instantly reached hundreds of millions of users. It’s estimated that the attackers earned around $120,000.

Twitter responded by temporarily suspending the ability of all verified accounts to post new messages and immediately launched an investigation. The company issued a statement on July 18 saying it believed certain employees had been socially engineered by attackers who used those employees’ credentials to access Twitter’s internal systems and from there initiate password resets, log into the accounts, and send Tweets that appeared to be from the hacked celebrities.

At this time, few details are available from the investigation, so it’s unclear what exactly Twitter means by socially engineered. The company could be referring to any one of a number of tried-and-true tactics that convince employees to let down their guard, due to a lapse in judgment or a lack of training, and unintentionally provide access to an attacker—for example, by opening a door to a restricted area to let someone in without first checking if they have an access card or company ID; plugging a USB stick that was mailed to them into their work computer to check what’s on it; or clicking on a link in an email and inputting their username and password on a phishing site.
4 Tips for Safer Credit Card Use

SOME OF THE LARGEST credit card data thefts in history, including the 2013 and 2014 breaches at Target and Home Depot that resulted in tens of millions of cards being compromised, were perpetrated by hackers using software-based skimmers.

These skimmers target the software component of payment systems and platforms, whether that’s the operating system of point-of-sale terminals or the checkout page of an e-commerce website. Any software that handles unencrypted payment card details can be targeted by data-skimming malware.

Hackers gain access to these systems through stolen credentials or by exploiting vulnerabilities, and they install malicious programs that scan their memory for patterns matching payment card information. Card data, except for the PIN, is generally not encrypted when passed from the card reader to the application running locally, so it can be easily copied once identified in memory.

Consumers can’t do much to directly prevent such compromises because they don’t control the affected software—it’s the responsibility of the merchants and their technology vendors to provide a safe shopping experience. But you can take the following actions to reduce the risk that your own card will be exposed and to limit the impact if a compromise does happen:

1. **Monitor your account statements** carefully and often, and keep an eye out for transactions you don’t recognize. Call your financial institution immediately if you see evidence of unauthorized activity.

2. **Turn on transaction notifications, if your bank offers that service.** The sooner you discover fraudulent transactions and can replace your card, the better.

3. **Use virtual card numbers for online shopping if your bank offers them, or pay with your mobile phone.** Services like Google Pay and Apple Pay use tokenization, a mechanism that replaces the real card number with a temporary number that is transmitted to the merchant. This means your real card number is never exposed.

4. **Pay with an online wallet service, such as PayPal, that doesn’t require you to input your payment card details directly into the checkout page of the site you’re shopping on. You can also choose to shop only on websites that redirect you to a third-party payment processor to input your card details instead of handling the data collection themselves.**

What Type of Mobile User Are You?

HOW DILIGENT ARE YOU when it comes to mobile device security? If you recognize yourself among the four types described below, it’s time to re-evaluate your approach.

A. **THE UNSUSPECTING**
You’re not really aware of the dangers lurking online, so you aren’t concerned about protecting your smartphone or tablet. That makes you an easy target. Unsuspecting types fall for basic scams, willingly clicking on links in unsolicited emails and entering their IDs and passwords on unfamiliar websites when asked. But messages opened on mobile devices can infect laptops and company systems. Remember: Think before you click.

B. **THE DELAYED REACTOR**
When you misplace your tablet or smartphone, you hesitate to tell the IT department. After all, it’ll turn up sooner or later, won’t it? Maybe not. Next time you lose track of your device (if there is a next time), call your employer’s IT department immediately. Any lag time can put devices and sensitive personal and company information at risk.

C. **THE OVERSHarer**
You like to use your device to post personal and work-related information freely on various social media sites. Beware: You’re giving scammers a leg up when they try to infiltrate your company’s systems or steal your identity. They’ll use those details to help them pretend to be a co-worker or acquaintance, and they’ll try to persuade you to share credentials, passwords or other company data.

D. **THE TECH GENIUS**
You’re proud to be tech-savvy, and you should be! But if you’re not careful, you might turn into a security nightmare—especially if you know how to reconfigure your smartphone to give yourself administrator-level privileges. Doing that can turn a user into an administrator who can then access certain device resources that are normally inaccessible, and endanger data by removing important protections. They can also allow malware to be downloaded to the device and open it up to all sorts of malicious actions. The lesson here? Just because you can, doesn’t mean you should. If you try to bypass your company’s mobile device management tools, you may violate company policy as well as make your employer’s network vulnerable.
NEW SCHEMES FROM SCAMMERS

The pandemic has given rise to a host of new schemes from scammers. Be wary of unsolicited emails relating to COVID-19 in these areas:

» Charitable contributions
» General financial relief
» Airline and other travel refunds
» Sales of testing kits

In addition, be suspicious of anyone hawking products that claim to prevent, treat, diagnose, or cure COVID-19, and keep an eye out for counterfeit (and most likely ineffective) sanitizing products and personal protective equipment (PPE) such as N95 respirator masks, goggles, full face shields, protective gowns and gloves.

Experts Predict Ways Cybercrime Might Flourish in a Recession

As the world faces tough financial times ahead, how will cybercriminals react? During the 2008 recession, cybercrime increased: Regulatory Data Corp saw an average rise of 40% in cybercriminal activity for the two years following the recession’s 2009 peak.

But that recession occurred when cloud services and smartphones were still new, and cybercrime tools and services had yet to be commoditized. That’s why it’s hard to make predictions based on the 2008 recession, says Jeff Pollard, a principal analyst at Forrester. “We are much more dependent on technology than even a decade ago, so I’d expect to see cybercrime increase,” he says.

Here are some key areas to watch:

PHISHING

“When you have people uncertain as to what tomorrow is going to bring, we do certainly see an increase in fraud, largely associated with phishing attempts and social engineering campaigns,” says Deborah Golden, U.S. cyber and strategic risk leader for Deloitte Risk and Financial Advisory.

“We have seen a spike...of thousands of domains being registered with words like ‘stimulus,’ ‘relief,’ ‘refund’ and ‘rebate’ in them,” says Allan Liska, senior threat intelligence analyst at Recorded Future. “We’ve seen that rapid change [from COVID-19 emails] to, ‘Here’s how you get your check from the government,’ or ‘Here’s how you get a relief loan.’”

MORE PEOPLE USING HACKING TOOLS

In a recession, young people, especially those with IT skills, may turn to cybercrime, as has previously happened in countries such as Nigeria and Honduras. “High unemployment rates among young people in the developing world and limited job opportunities in the legitimate IT sector create push factors for ‘deviant globalization,’” according to a new report from the Global Initiative Against Transnational Organized Crime.

INSIDER THREATS

One trend from earlier recessions that experts say we’re likely to see again is problematic behavior from people within organizations due to fears over job losses, pay cuts or targets being harder to achieve. “Layoffs and furloughs always lead to a bigger concern around insider threat,” says Liska. “Going all the way back to the dot-com bust in 2000, we’ve seen it in the past that insider threat activity increased dramatically during those rounds of layoffs.”