https://www.darkreading.com/attacks-breaches/10-social-engineering-attacks-your-end-users-need-to-know-about--/d/d-id/1330171

10/19/2017
02:30 PM

Steve Zurier

10 Social Engineering Attacks Your End Users Need to Know About

It's Cybersecurity Awareness Month. Make sure your users are briefed on these 10 attacker techniques that are often overlooked.

It's the middle of National Cybersecurity Awareness Month: the perfect time to look beyond the obvious stolen passwords, phishing and malware, and into some of the social engineering attacks less known to the average end user. And here's something you security professionals might not know: 43 percent of breaches in the last year were related to social engineering attacks, according to the Verizon Data Breach Investigations Report.

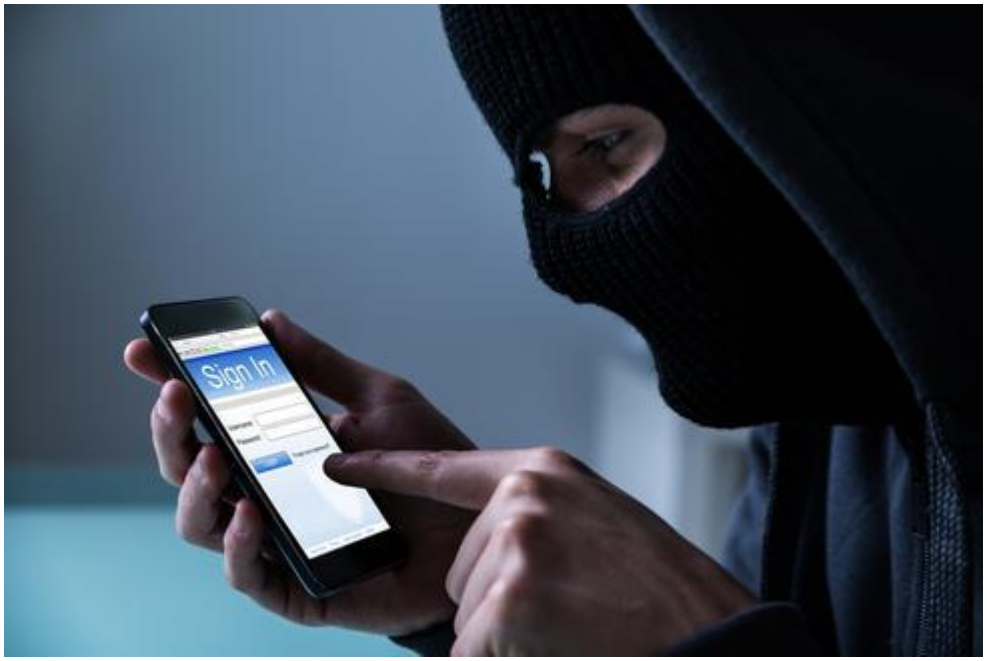
"We're seeing a lot of social attacks, especially taking advantage of lonely guys at home," says Aaron Higbee, CTO at PhishMe. "Attackers will entice a person with a nude picture then get him to send a nude picture of himself. Then the attacker will say they will send it to Facebook unless they pay a ransom."

Christopher Hadnagy, chief human hacker at Social-Engineer adds that people should be aware that social attacks such as phone-based vishing where attackers try to steal money over the phone are becoming more prevalent.

"Criminals buy data on the Dark Web then call people saying they owe several thousands of dollars in back federal taxes from a few years ago." Hadnagy says. "Even though people may know that the IRS will only notify them in writing and will never call them directly, they still fall for it."

Based on interviews with Higbee, his colleague and chief threat scientist at PhishMe, Gary Warner, and Social-Engineer's Hadnagy, Dark Reading has developed a list of 10 hacks that might not always be as readily apparent,

1. Vishing



End users are so focused on looking for fraudulent emails that many forget hackers often prefer to go low-tech with voice, or vishing calls.

In some of these phone calls, scammers purport to be Microsoft support and ask the user to give them their credentials and/or their credit card. Never do this. Remember that NO ONE from Microsoft will ever call you out of the blue asking how your computer is doing. The same holds true for the IRS, but people fall for it. Scammers call people all the time and tell them they may owe something believable, say $3,000 in back taxes for 2012. Once again, this will never happen. The IRS won't call you and won't send you an email. For better or worse, they will only communicate with taxpayers about back taxes in writing. If you receive a fake Microsoft Tech Support call, report it: https://www.microsoft.com/en-us/reportascam/.

2. Attackers using SEO to scam legit web users

Do you have an old printer or scanner you need a driver for? Watch out, because for a few dollars attackers can use marketing tactics to drive search engine traffic to a fake driver that infects your computer.

For example, based on your search for help with printing it may take you to a website that looks like it has official drivers, but instead serves infected malware. They don’t have to spend a lot of money to build a website and purchase key Internet search terms to lure unsuspecting victims.

3. Phishing websites can be HTTPS

The conventional wisdom was that SSL on a HTTPS site is a sign that it’s safe. Attackers didn’t want the headache or expense of obtaining a valid SSL certificate, which made them extremely rare. Not so anymore, thanks to websites like letsencrypt.org, which give away free SSL certs.

Users cannot assume a site is safe because of HTTPS. For important banking and other log-in pages, they should "look for the green bar" which means the site is not just using HTTPS, but is using an Extended Validation SSL certificate (EV-SSL), which bad guys cannot get for free.

4. Phony sites filled with malware that appear like real ones

People browse the web freely and aren't always paying close attention. Hackers can register a domain name of a legitimate website such as PayPal or eBay and make them look nearly 99 percent authentic. Clever fraudsters hide malware on these pages and also hide foreign language characters that aren't readily visible to the naked eye unless the person works as a late night copyeditor.

5. Right-to-left override

While it’s been around for a while, users should also be aware that hackers can use a “right-to-left-override” to launch malware. What happens is that a file will look like this: validate.exe.jpg, basically a normal jpg file. But in reality, using Unicode, an international translation system, the file is actually an executable named validate.jpg.exe. The user then unknowingly launches the malware, infecting the computer.

Reiterate the golden rule: If you weren’t expecting the file from that person, don’t open it.

6. Embarrassing selfie ransoms and porn site unsubscribe scams

For these lures, the targets are typically lonely men. A fraudster sends a nude picture of a woman enticing the victim to send back a nude picture of himself. If the man takes the bait, the fraudster then sends back a ransom threat, saying they will post the photo on Facebook or other social media unless they pay the ransom.

These types of crimes are low tech, the fraudster doesn’t even have to write code or set up a website. All they really have to do is have a few .jpgs of nude women. In another sex scam, users get sent a porn site at work telling them they are subscribed. To unsubscribe, they are asked for their work emails and passwords. People take the bait and all it takes is one weak person to give away the keys to the corporate kingdom.

7. Low Tech Ransomware

As just discussed, some attackers go low-tech. For this lure, the attackers send the user an email that their files were hacked and that the hackers gained access to corporate accounts. Of course, this is a complete bluff, but usually the hackers ask for $300 (USD) worth of Bitcoin.

A worried end user may pay the ransom just for peace of mind. In this case, all the hacker needs is an email address and they can make some quick money.

8. “File Too-Big” phishing emails via DropBox, Box or OneDrive

Have you ever tried to attach a file to an email but were told the file was too big? People have grown used to sharing larger document files and video via Dropbox, Box or OneDrive. In this lure, the attackers will send the victim an email that looks like it’s from a colleague or a supervisor and tell them to take a look at the document, presumably from an ongoing project. Using this method, the attacker can circumvent email security protections and get the victim to open the malware hosted on a popular file-sharing site.

9. Gaining administrative access

Security professionals know that attackers have many ways of using "lateral movement" to reach their target, but highly privileged end users don't always realize they will be attacked via others in the company.

Access to HR databases or wire transfer privileges might be obtained this way. Or a hacker may want an IT helpdesk worker's admin access rights. So the attacker may access a user's machine then purposefully break something or send a ticket to the help desk that says an app such as Word has been disabled on their machine. When the help desk person logs in, the hacker then steals the cached administrative credential, giving him access to the corporate network.

10. Automated tools that hack through any word

Attackers have automated software that checks passwords for every word in the dictionary – so using ANY word or name in a password reduces security. It's not a matter of being "guessable or not guessable" – users need to focus their passwords on letters and numbers that make no sense and wouldn't be found in any dictionary (or phone book).

https://www.darkreading.com/author-bio.asp?author_id=2460

Profile of Steve Zurier

Freelance Writer News & Commentary Posts: 91

Steve Zurier has more than 30 years of journalism and publishing experience, most of the last 24 of which were spent covering networking and security technology. Steve is based in Columbia, Md.