PHISHING: Know Your Technology!

I received a call today from a bot reporting itself as Amazon and alerting me that a $1,000+ charge had been made on my Amazon account for a new iPhone 11 and to press “1” for a rep to discuss this charge. Naturally, I pressed “1” to play along and see where this went. I was transferred to an agent purporting to be an Amazon customer service rep. He asked me if I wanted to receive the phone and was surprised when I answered “hell yeah” since they’re expecting you to be shocked by this order and to scare you into giving up personal information or remote access to your computer.

When I answered yes, he proceeded with shipping information. Is this going to “Ken Carmack?”

ME: “Yes”.

REP: “ Is the address 167…”

ME: “No, that should be 167 Main Street”

REP: “OK, is that going to Raleigh?”

ME: “No, it should be Wilkesboro”

By then, he knew that he was being played and disconnected.

The bottom line here is that phishers are constantly whipping up new schemes such as this one, to scare you into thinking that you’ve been charged for a TV, iPhone, Norton antivirus or similar. In your panic, they hope that you will divulge personal information or provide access to your computer which they can then exploit.

A common tactic that I’m seeing lately are emails with an invoice or payment confirmation stating that your account has been debited $389.99 for McAfee or Norton renewals and to call their 800 number if you need assistance or have questions. One client of mine was scared into action by this, dialed the 800 number and provided remote access to his computer to an “agent”. BOOM! A win for the attacker!

Another common tactic is an email from “Microsoft” warning that the password to your Microsoft account is expiring in short order. The goal here is for you to click on the link, proceed to a page that **looks** like Microsoft where you enter user credentials which they can then use to login in to your actual Microsoft account. These emails sometimes look like they originated from Microsoft but are often sent from an email account or domain that bears no resemblance to Microsoft, such as billy@wescammedyou.com.

So how to spot/avoid phishing tactics? There are several red flags or rules of thumb to keep in mind:

1. **KNOW YOUR TECHNOLOGY!** Are you using McAfee or Norton, such that a renewal is in order? If not, don’t take the bait. Most of my clients use BitDefender so be aware of your security suite. I never use McAfee or Norton unless a client has purchased that on their own. Nevertheless, you should be aware of what is protecting your computer, not only to ensure you’re protected, but also as a defense against phishing.
2. **Does the sender’s email address resemble the soliciting company?** For example, one McAfee renewal that I reviewed came from an @gmail.com account which raised a red flag. If the sender’s address is hidden, hover over the sender name/address to see the underlying sender’s account. If the sender presents as Microsoft, see if the underlying email address is actually @microsoft.com. While this is not foolproof, you can quickly rule out many bogus emails that arrive in your inbox.

3. **Does the invoice address you by name or company name?** If the renewal is addressed to “Dear Customer”, then they probably never had the original subscription.
4. **Is your address or last 4 digits of your credit card referenced?** Once again, vague invoices/confirmations with scant specific details are a red flag.
5. **When in doubt**, send the items to your IT department to verify for legitimacy.
6. **Under no circumstances should you reply to the email or call their 800 number.** If you’re legitimately concerned that you’ve been charged, then log in to your banking or credit card account and scan for pending or completed charges. If the caller or email claims that the purchase was made in your Amazon account, log into that account and review your orders. When accessing financial or online accounts **NEVER, EVER click a link in an email**. Always open your web browser and navigate to your accounts as you normally do. *Links in emails can send you to web pages that look like the real website but are designed to collect your user credentials.* Also, enable 2 factor/multifactor authentication on accounts that contain financial or sensitive information.

One more phishing story and I will get back to work. A few months ago a client called and stated that their company’s president’s (let’s call him “Fred”) phone had been hacked. A young employee (call him “Jimmy”) in the company received texts from the president asking him to run an errand and buy 15 @ $100 Apple gift cards to distribute to the staff as performance awards. Oh, and don’t bother calling Fred because he’s in meetings and using someone else’s mobile phone since his battery is dead. Long story long, Jimmy followed the instructions to the tee, purchased the cards, scratched off the backing, shot photos and texted the images to “Fred’s” phone. BOOM!

Bottom line, Fred’s phone was never hacked. It was probably a burner phone that got trashed immediately after the successful caper. Further, my client contacted Apple to deactivate the gift cards. I suppose that’s possible, but the hacker knew that time was on his side and wasted no time spending them. Jimmy was out $1,500 at the end of the day.

A few key rules of thumb that could have prevented this hack:

1. **Verify the sender using a different communication method**. Don’t **text** Fred back to ask if it’s really him since the attacker will respond affirmatively. Call Fred on his landline or send an email. I have seen successful attacks where the hacker emailed the victim, the victim verified via the same email channel and the attacker confirmed “yeah, this is legit!”
2. **Run a smell test**: Does this make sense for the president to reach out to a new employee for an errand like this? If you don’t have the experience/context to answer that question, check with your peers. If Fred is really in a meeting, what’s a few minutes to ask around to confirm that. Remember, these hackers use fear to kick you into quick action, which always works in their favor.
3. **Avoid mobile numbers on your company website.** If you want to post phone numbers, add landlines that cannot receive texts. You can config most landlines to forward to a mobile phone so that you don’t miss calls. Many phishing attacks are via text message, so posting your mobile number on the web provides a very easy target.
4. **When in doubt: DON’T!**

Over the years, we’ve all learned to ignore and delete emails from Egyptian pharaohs, lottery winnings, and all the other too-good-to-be-true trickery. However, scammers are getting more clever, so it pays to be cautious and dial up your BS detector.

Be careful out there!

About the Author: *Ken Carmack has over 20 years of experience in the technology field and provides onsite and remote services for a broad range of IT needs. A former CPA, Ken knows what a business needs, and can help you meet your financial and productivity goals. Partner Technology Solutions, LLC specializes in IT support for small/medium businesses in the Raleigh, NC area. We offer onsite support, remote assistance, training and drop off services.*