IT Pros: Protect Your End Users from These 7 Notorious Online Scams

Devolutions

THERE IS A STRONG POSSIBILITY THAT CYBER CRIMINALS WILL GET A HOLD OF DATA THAT WILL ALLOW THEM TO BREAK INTO THE CORPORATE NETWORK

As an IT pro, you're probably very capable of steering clear of online scams. However, your non-technical end users may not be so fortunate. And if they get hacked on their personal device, there is a strong possibility that cyber criminals will get a hold of data that will allow them to break into the corporate network — which will put everyone at risk, including your customers.

To prevent this nightmare from happening, below we highlight **7 notorious online scams** and how to avoid them. We encourage you to send this article to your end users so they can be part of the security solution — instead of unintentionally finding themselves at the root of the problem:

1. Tech Support Scams

Tech support scams start with a phone call, email, pop-up message, or online ad that lures potential victims into fixing an urgent problem that doesn't exist – like, say, a security vulnerability. And because payments for these support services are typically made by wire transfer, bitcoin, or by putting money on a gift card, it's virtually impossible for victims to reverse the transaction once they realize what has happened.

How to Avoid this Scam: First off, no legitimate company will — out of nowhere and without being asked — scan your computer and tell you something is wrong. Second, if you suspect there might be a problem with your computer, you can always update your security software and run a scan to see what's going on. And finally, if you need help fixing a problem, contact a legitimate specialist or company you know and trust.

2. Online Shopping Scams

Online shopping scams use fake websites that look legitimate and authentic. They often (but not always) offer premium and luxury goods at extremely low prices – like high-end laptops, cameras, jewelry, watches, designer handbags, and so on. As with the tech support scam, fraudsters typically require payment through wire transfer, cryptocurrency or pre-paid gift cards. Unfortunately, such offers are too good to be true. At best, victims end up with counterfeit goods that either don't work or are virtually worthless. But most of the time, they don't get anything and wind up losing their money.

How to Avoid this Scam: Before purchasing any item online, make sure the site is secure (HTTPS). You should check for reviews on Google and other third-party platforms. It's also wise to email the seller first to make sure they respond (and the email should of course come from a business domain). If you decide to move ahead, consider making a small purchase first to make sure everything runs smoothly. And under no circumstances should you ever pay through a wire transfer or by pre-loading a gift card. As noted above, it's virtually impossible for these transactions to be reversed.

3. Lottery Scams

Who hasn't dreamed of winning the lottery and living the good life? Unfortunately, scammers tap into this fantasy by telling victims that they've won a massive amount of money — usually in the millions of dollars. Typically, such scams then ask you to confirm your name and address, and to send your bank account and/or PayPal information to claim their money. Invariably, there is no such lottery, and the end result is that fraudsters use the data to commit identity theft. In some cases, victims are told to pay a small processing or handling fee, which only adds to their loss and misery.

How to Avoid this Scam: First of all, if you didn't enter a lottery, then you simply can't win. That's pretty straightforward. But let's say the email you get is extremely convincing, and perhaps you do vaguely recall buying a lottery ticket a while ago. In that case, you need to be highly skeptical. If you're asked to pay a fee of any kind, then you know it's a scam. You should also Google the lottery — in most cases, you'll quickly see that it's a scam. And if you want to contact the organization, look for their contact information through another source. Never ever call the number in the email. If you do, you will fall right into the trap they have set for you!

4. Bitcoin Scams

Scammers love bitcoin. Or rather, they love victims who fall for common bitcoin scams like fake bitcoin exchanges, Ponzi schemes, fake bitcoins, fake ICOs, pump and dump, bitcoin gold scams — the list goes on. While each scam has its own methods and tactics, the basic story is the same: victims don't do their research and end up losing anywhere from a few hundred to millions of dollars. For example, in 2014 Bitcoin Savings and Trust was fined $40.7 million US by the SEC for creating fake investments and building a Ponzi scheme to scam investors.

How to Avoid this Scam: The bad news is that there is no single, straightforward way to avoid bitcoin scams — simply because there are so many out there. However, you can dramatically reduce your risk by doing your research and double-checking all sources. To head in the right direction, check out this helpful article by Investopedia, which offers advice on avoiding different bitcoin scams.

5. CEO Fraud Scam

First of all, a CEO fraud scam is not about replacing a legitimate CEO with a fake one. Rather, it involves a short message from the CEO to an employee asking about a payment. It could look something like this email, which was actually taken from a real CEO fraud attack and published by the cybersecurity company Trustwave:

From: John Smith Sent: Monday, 13 November 2017 11:27 AM To: Susan Brown Subject: Urgent Attention

Are you available to handle an international payment this morning?

Have one pending, let me know when to send bank details.

The victim who receives such an email believes they are communicating with the real CEO, and so in most cases they stop what they're doing, pay attention, and carry out the order. If they don't reply promptly, the potential victim often gets another, somewhat agitated email telling them that time is of the essence and they need to transfer funds. This continues until the victim complies. And if you think that CEO fraud is small scale, then think again! In 2015, cyber criminals used a CEO fraud attack to steal more than $3 million from Mattel.

How to Avoid this Scam: To start with, companies should have a multi-step approval process for large transfers, and all transfers (regardless of amount) should be validated with a purchase order or some other proper documentation. It's also vital for companies to continuously educate their employees on how to spot and avoid scams, both when they are at work and when they are at home.

6. Sextortion Scam

The sextortion scam starts with a long, sloppily-written, scary email that tells victims about hackers who have filmed them (through their own web cam) browsing pornographic websites, and that videos and/or photos will be published publicly unless victims make a bitcoin payment right away (usually in 24-48 hours). What's more, hackers behind sextortion are now starting to include the victim's own email account password as proof that they have been hacked. Here is an example of a sextortion email published on www.actionfraud.police.uk:

I'm aware, XXXXXX is your password. You don't know me and you're probably thinking why you are getting this mail, right?

Well, I actually placed a malware on the adult video clips (porno) web site and guess what, you visited this website to experience fun (you know what I mean). While you were watching video clips, your internet browser started out working as a RDP (Remote Desktop) with a key logger which gave me access to your display screen as well as web camera. Just after that, my software program gathered every one of your contacts from your Messenger, Facebook, and email.

What did I do?

I made a double-screen video. First part shows the video you were watching (you have a nice taste omg), and 2nd part displays the recording of your webcam.

Exactly what should you do?

Well, I believe, $2900 is a fair price tag for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).
BTC Address: 1HpXtDRumKRhaFTXXXXXXXXXX

(It is cAsE sensitive, so copy and paste it)

Important:

You now have one day to make the payment. (I have a special pixel within this email message, and now I know that you have read this e mail). If I do not receive the BitCoins, I will definately send out your video recording to all of your contacts including close relatives, co-workers, and many others. Nevertheless, if I receive the payment, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I will send your video to your 10 friends. It is a non-negotiable offer, therefore do not waste my time and yours by responding to this message.

The good news is that this is a scam. Hackers don't have videos and photos of victims. The bad news, though, is that many people fall for this and end up paying.

How to Avoid this Scam: Don't reply to the email whatsoever, even to ask a question. Replying sends a signal to the hackers that you may be vulnerable. You should also enable 2FA on all of your accounts (not just email), and always use strong passwords that are at least 11 characters in length (passphrases are even better). If you suspect that your password has been breached, then change it immediately, and store your passwords in a secure repository vs. spreadsheets and text files.

7. Greeting Card Scam

Greeting card scams have been around for a long time, and they continue to thrive for the simplest and most unfortunate reason: they work. It all starts with a victim receiving an email greeting card, typically around a holiday like Christmas or Easter. However, once they open the email and either click on a link or download an attachment, they end up infecting their computer with malware. At best, the malware pesters them with pop-ups and ads. At worst, hackers get unlimited access to their system and wreak havoc.

How to Avoid this Scam: While it's always nice to get a greeting card, be very suspicious about clicking on any link or downloading an attachment. If the email is from someone you know, then contact them directly (not by replying!) and ask them if they've sent you a greeting card. Also, don't be fooled if the email has your full name. Hackers can easily use a program that captures your display name and puts it in their email template.

From the Desk of Our (Real!) CSO Martin Lemay:

"A security awareness program does not provide any guarantee that an organization's staff is bulletproofed against scams. While it reduces the likelihood of compromise, someone will most likely get caught one day. It is therefore vital to have resources ready to listen to victims and help them out. It is also important that the organization does not punish victims for falling into those scams. A better strategy would be to reward them when incidents are reported in a reasonable timeframe. That way, the business encourages its staff to report incidents, allowing the organization to respond quickly to security threats."

The Digital Road Ahead

We all know that cyber criminals are not going to slow down. All they need is a very small percentage of victims to get snared by their online traps, and they can make massive amounts of money. Educating your end users is critical to ensure that the digital road ahead for them — and possibly for your whole organization — is safe instead of scary.

Your Input

What online scams have you encountered — either in your personal or professional life? Please comment below, and also share your recommendations for staying out of harm's way.