IT Pros: It's Time to Warn Your Users About the Dangers of Online Shopping

Devolutions

HACKERS ARE AGGRESSIVELY TARGETING ONLINE SHOPPERS IN ORDER TO BREACH DEVICES, STEAL DATA, AND DEPLOY SPYWARE!

As an IT pro, you've probably spent many hours educating your users on cyber security best practices, such as always choosing strong and unique passwords, never sharing account credentials, saving passwords and other confidential data in a secure repository rather than using spreadsheets or sticky notes, and so on.

However, there is another lesson you should add to your teaching curriculum as we shift from Black Friday/Cyber Monday territory and into the frenzied Christmas gift-buying season: the dangers of online shopping.

No, this has nothing to do with keeping your colleagues from spending a fortune on collectible Furbies from eBay. This is about making sure your users understand that hackers are aggressively targeting online shoppers in order to breach devices, steal data, and deploy spyware — which could ultimately lead to an attack on the corporate network.

To avoid this nightmare — according to IBM Security and Ponemon Institute, the average cost of a data breach has climbed 6.4% from last year to a whopping $3.86 million per incident — here are four key lessons your users need to know when it comes to online shopping, both for their protection, and to protect the organization as a whole:

1. Beware of offers that seem "too good to be true"

Some offers are great, such as our Cyber Monday deal where you can save 50% on a Remote Desktop Manager Single License. But others are just plain crazy, like the one floating around out there that claims to offer 99% off purchases at Amazon. Unfortunately, victims who fall for these scams end up sharing personal and confidential information with hackers.

The lesson for your users: If an online shopping offer seems "too good to be true" then it probably ISN'T true! At the very least, users should contact the seller directly to confirm the offer. Better safe than sorry.

2. Check and confirm valid security certificate (HTTPS)

Hopefully your users know that when they're online shopping through their desktop, they should always check their browser address field and confirm that a site has a valid HTTPS connection. However, mobile browsers use a shorter address field. As such, the HTTPS doesn't typically appear — which means the site may or may not have a valid security certificate. According to research by Panda Security, each week hackers create a staggering 57,000 new URLs that they position and index on search engines to lure unsuspecting victims.

The lesson for your users: Before visiting a site when using a smartphone or tablet, ensure that it has a valid HTTPS security certificate. Don't assume that it does.

3. Be extra careful when downloading apps

We all know the old iPhone commercials that told us, regardless of what we need, "there's an app for that". Well, unfortunately hackers got the message as well — because they have created thousands of bogus apps to steal identities and data. In fact, according to a recent report by RiskIQ, 5.5% of Black Friday-related apps in global app stores are malicious and 4.6% of Cyber Monday-related apps are malicious.

The lesson for your users: Be very careful before downloading apps — even if they seem harmless, like one that is trying to help you get some great online shopping deals. And while it's relatively safe to download apps from official sites like Apple's App Store and Google Play, it's still important to exercise caution.

4. Watch out for email links and attachments

There's nothing new about hackers trying to "phish" for victims through email. They've been doing it for decades. However, many people assume that an email from a store or retailer they like — such as Apple, Amazon, eBay, and so on — is safe. Unfortunately, this isn't always the case, which is something that victims discover too late.

The lesson for your users: Scrutinize all incoming emails and think twice about clicking links, especially when downloading attachments. If possible, it can be safer and wiser to browse to a company's website and see what they have to offer instead of clicking a link in an email.

5. The Bottom Line

Ultimately, all of the above lessons for your users — along with these tips for safer online shopping — are part of a larger message: cyber security is not only something users need to pay attention to when they're at work. It's something they need to be committed to and vigilant about AT ALL TIMES, including when they're at home and using their personal devices.

Why is this so vital? Because they aren't the only ones at risk! If they get hacked — which can happen without their knowledge — they could endanger and damage the entire organization.

Simply put, to stay a step ahead of the bad guys, everyone must be part of the cyber security solution at work, at home, and everywhere else.