For Oklahoma Bankers Association
Rayleen M. Pirnie, AAP
RP Payments Risk Consulting Services, LLC

Business customer article

What you need to know about Do-Jacking

It's probably no surprise to you that criminals go to great lengths to scam the unsuspecting. This form of fraud has been around for a long time, but we're seeing more incidents of it in recent months. Do-jacking relies on a simple typo to download nasty malware on your computer, on a site counterfeited to look like your bank.

Domain Jacking (do-jacking for short), also called typo-squatting, uses slightly different versions of a legitimate website, hoping you make a typo while trying to get to the bank's site. For example, instead of "bank" the criminals may register a domain with "bnak" hoping to snag someone who simply typed the letters in the wrong order.

Other common methods involve registering domains using .cm or .co instead of .com. For example, "myonlinebank.co" instead of "myonlinebank.com." This method is also common in what is called click-jacking; criminals send you a fake email, claiming to be your bank, and urge you to click a link to connect to the site. But you aren't headed to the bank's real site if you do click the link.

Once they get you onto their fake website, a few different things can happen. One, if you try to log in to what you think is your online account, then the criminals can take your credentials and use them to initiate fraudulent transfers. You will just see an error message that the site is down or experiencing problems, and to try again later. Remember, you're not actually on the bank's website at this point.

A more common method to this scam is the use of some notice about outdated security on your computer, or the need to download Adobe Flash. Once you click "agree" or "download now" to the required update, adware or financial malware downloads on your computer.

What do my employees need to do to avoid Do-Jacking (and other cyber-frauds)?

1. Type website addresses carefully. Double check the address before hitting enter.

2. Bookmark legitimate websites so you can use a bookmark to connect vs. typing the link. This will help you avoid future typing errors.

3. Don't click on pop-up warnings. Personally I suggest you never click on them, even if you are on the correct website. There are other frauds criminals use on legitimate websites that infect your computer, almost always using a pop-up alert of some kind. If you need to download a program or update your security, go

directly to the provider’s website. I am personally not aware of a single legitimate time when a bank’s online banking site used a pop-up indicating an update to your security was required. These have always been found to be fake.

4. If you receive an email from your bank, don’t click the link in the email. Go directly to the website by typing it into the browser yourself or using your own bookmark. The email may not actually be from the bank.

The internet is a vast world, filled with good sites and bad ones. A simple wrong letter can lead you to a disastrous detour. Safe surfing my friends.

About the Author

Rayleen is the CEO of RP Payments Risk Consulting Services, based in Orrick, MO. She travels the country presenting at fraud, payments and security conferences on topics ranging from Mobile, fraud, payments risk management, and information security. Previously she was the Director of Compliance and Fraud at a regional payments association for 8 years, and worked financial crimes investigations for a community bank for 7 years. Rayleen has been writing and presenting for over 10 years.