The Millennial Minute

Fake CAPTCHA Scams – What are they? How can you protect yourself?

BMO | Private Wealth

Written by Ashley Nichols – Client Service Associate for the Biddle Wealth Management Team

If you've used the internet at all over the last decade, you've run into CAPTCHA prompts. We've all encountered them. They're those fun little puzzles you must solve like: "Enter the swirly letters and numbers you see on your screen", or "Click the images until there's no more bicycles left". (Side note: I get tricked every time they put a blurry motorcycle in the mix – I think that's just dastardly.)

CAPTCHA is an important security tool used to authenticate that you are, in fact, a real person. These little tests are things that humans can solve easily (unless there's motorcycles, apparently), but automated programs find difficult. CAPTCHA assists with keeping websites safe from spam and fake accounts.

So, how can scammers use CAPTCHA to cause harm?

It's as simple as taking advantage of our comfort and trust. We are so used to seeing these CAPTCHA challenges – especially the all-too familiar "I am not a robot" box that you can easily tick off and be on your merry way, that we forget we use them almost daily. Criminals have caught on to that comfort and can lure people to fake websites and give it an air of legitimacy by having a fake CAPTCHA. Sometimes scammers copy well-known brand sites and give them a subtly different web address, and the add a fake CAPTCHA to it to put malware on your device. Some pages can copy a CAPTCHA so closely that we potentially won't even think twice about completing it.

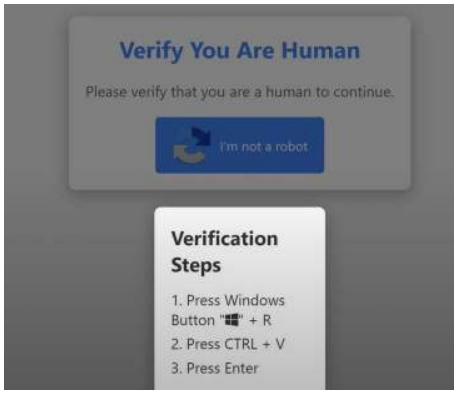
DID YOU KNOW? CAPTCHA is used by more than 11 million websites (according to BuildWith.com)

So, how does a fake CAPTCHA scam work? And how does it harm us?

Fake CAPTCHA can take different forms. The most common is a fake CAPTCHA that claims you must complete additional verification. The page will automatically copy a malicious command to your clipboard and then asks you to "run it" in the Windows Run dialog box (Win+R). This can then install information stealers that can take your passwords, browser cookies (these store personal information like login statuses, completed online forms, your

internet preferences, and they also track your user behaviour for marketing purposes); it can even allow attackers to browse your files or open backdoors into business networks.

CAPTCHA scams can be very sophisticated. Here are some common ones you might see:



The scams that are harder to spot will typically request more from you for 'verification'. They may ask you to download files or enable notifications. If a CAPTCHA asks you to paste a provided code into your computer, this is a huge red flag, and you should leave that site immediately. Fake CAPTCHAs often end up on unfamiliar or suspicious-looking domains. If the domain is a complicated web address such as: **js3820_xxZhry.strangesite-name.yzx**, then you should NOT automatically trust it. Fake or unofficial sounding domains are the number one red flag to look out for!

CAPTCHAs also rarely show as a pop up. They will either be at the bottom of the web page, or load as a new webpage before continuing.

Of course, we all fall victim to scams. **What do you do if you've clicked on a fake CAPTCHA?**

While you don't need to set your computer on fire, you need to act fast. Close your browser tab immediately, fully disconnect that device from the internet and run a full antivirus scan to limit any damage.

When running anti-virus software, you should always ensure it is up to date so it can detect the newest threats. If the scam prompted you to download a file, DELETE IT! Do not open it as it can run harmful scripts. Once you delete it, empty your trash/recycle bin so it's gone for good.

Next, clean your browser by clearing cache, cookies, and removing extensions you don't recognize. Some fake CAPTCHAs attempt to plant malicious add-ons that survive even after you've left the site.

Once your system looks clean, change your passwords for your most sensitive logins, but do so from another device. Now is not the time to take chances! If you reuse passwords anywhere, now is a good time to update them. Malware often targets your saved credentials.

Over the next few weeks, monitor your accounts closely! Watch for suspicious sign-in notifications, unexpected messages on social media or notifications from your 2-factor verification apps. Attackers will typically wait a while before using your stolen data in hopes that you've let your guard down.

Good security device also adds another layer of defense. Keep your operating systems and antivirus software up to date so they can block new threats. Many security programs can actually scan pages for suspicious scripts before you interact with them. Some browsers can even include built-in protection against harmful code, like Google Chrome.

You can take further steps, like limiting or even disabling the 'Windows Run' dialogue box (Win+R). You can use script-blocking extensions or turn off JavaScript on risky sites.

CAPTCHA scams are becoming increasingly common. They're trusted and you don't need a lot of technical skills to create one. Unfortunately, Malware-as-a-Service kits provide ready-made scripts. All you need is your wallet and you too can run a CAPTCHA scam.

Industries that are rich in data or assets are the most attractive to these scammers. Online stores are especially attractive for their payment details. Online gaming platforms also hold accounts linked to your payment information – like online gambling sites. Any site where someone can log in and move money is a tempting target.

It's important to always be wary of your online presence. Be mindful of the sites you visit, the information you provide, whether or not you've saved passwords for certain sites and slow down on any 'mindless clicking'. Most scammers are betting on our ignorance and trustworthiness in order to get what they want. With a bit of knowledge and patience, you can lower your risk considerably.

***This information was taken from an article on CAPTCHA scams at Malwarebytes.com/cybersecurity. Their site has amazing articles to read further into different types of scams and dangerous activity found on the web.**