INSIGHTS

Cyber made simple.

one brightly cyber

YOU CLICKED THAT LINK

BY JAY BORDEN

We have all heard about phishing, emails that look real and ask you to click a link to provide private information. Maybe they appear to come from a business executive, a government agency or other "authorized" party. Or maybe they simply offered a great deal on something you wanted.

Not clicking the link is the best protection, but what if you did click the link?

You are not alone! Recent research shows 71% of respondents acknowledged doing something risky. How was something risky defined for this survey? As reusing a password on more than one site or connecting to a business site with a personal device not having the same protections as business devices. Or clicking a link or downloading an attachment in an email.

Better to be safe than sorry. Change your password. Change it on every site where you used it and do not use the same password on more than one site again. Let a password manager create the passwords. They will be long and complex. More difficult to guess or crack than what you can come up with in most cases.

Run a complete scan on your device using anti-malware. If you do don't have anti-malware on your device install it immediately. It is not expensive and effective in helping keep you safe. But won't always help against phishing.

Using any device, desktop, laptop, tablet, or mobile on the internet without anti-malware is just asking for trouble.

Clicking the link or downloading the attachment in a phishing email will install malware on your device. The malware will steal your credentials and more, then look to spread to other devices. Once a cybercriminal gets any of your credentials they will continue to attack to get more. Your password will be tried on multiple sites to see if it was used elsewhere.

onebrightlycyber.com
(888) 773-1920

YOU CLICKED THAT LINK

CONTINUED

Variants of the captured password, that is, changing a letter or a number or a special symbol will be tried because so many people think that is a new password. It isn't!

If you think there is the slightest chance your social security number was captured call the 3 major credit reporting agencies, Experian, Equifax, and Transunion. Ask that a credit hold be put on your account. Then no one will be able to request new credit cards, get a loan or take any other action that requires a credit check.

Also ask about being notified if any requests for a credit check come into the agencies. If it does then you know someone is trying to use the stolen information.

Along with notifying the credit reporting agencies, keep a careful watch on your credit; your credit card bills, bank accounts, store credit account bills, etc. Cybercriminals may charge things to your accounts or sell your credentials to others who will run up charges.

Multi-factor authentication, MFA, will add an extra step to logging into a system, application or anything. But it is worth it. MFA adds a layer of security that helps protect your accounts and information. Use it where ever it is offered.

If any of your private information was compromised report it to the FBI. If the compromise occurred on a business account regardless of whether you were using a business or personal device, report it to your Chief Information Security Officer immediately. If your company doesn't have one, then report it to the head of IT.

If your device shows any sign of problems, new software being loaded such as applications you don't recognize, slower performance, being redirected to different websites from what you entered, report it your IT department immediately. If it is a personal device, begin by reloading the operating system.

Yes, that will take time. But it is better than having your identity stolen and having to reclaim it and your credit.

YOU CLICKED THAT LINK

CONTINUED

Lastly, if it is a business device, ask your IT department to reset or delete any session cookies. Session cookies provide access to any system or application you have access to. This is a necessary step because the session cookies will still provide access even if the password is reset and the operating system reloaded.

Many people, including IT people, fail to take this step leaving a door wide open for cybercriminals to continue to access your systems and steal information or spread malware.

Yes, these all take time and effort, but ignoring the problem will not make it go away and the longer attackers have access, the more damage they do.

If you are a small company, consider outsourcing your security to a reputable firm that can monitor and manage your systems and devices.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.