Are You Being Hacked? 10 Signs to Watch For

Devolutions

SOME PRACTICAL ADVICE ON WHAT THEY SHOULD DO IF THEIR COMPUTER AT HOME HAS BEEN HACKED

Recently, I posted an article covering the 10 signs of a hack. It was designed for IT pros to share with end users, so they could be proactive vs. reactive.

This new article is also for end users, and offers some practical advice on what they should do if their computer at home has been hacked. Please feel free to share this with your team so they can stay safe at all times, and not just at work (and hopefully avoid calling you at 2:00am screaming “HELP! I'VE BEEN HACKED!”).

Dear End User:

Uh oh — after avoiding various attacks over the years, you've finally been hit and now the nightmare begins. No, I'm not talking about the Demogorgon hunting you down. This has the potential to be much, much worse. You've been hacked!

Obviously, this is the last thing that you want. But as scary as things are, it's really important that you stay calm and focused. Time is of the essence, and you need to act right away to mitigate the damage.

So, take a few deep breaths, brew some herbal tea, hug a puppy – it really helps:) – and get ready to take back what is yours. Here are the 7 steps to follow:

1 DISCONNECT YOUR COMPUTER

As soon as you realize that something is wrong, immediately disconnect your computer from all networks, and then **turn off the power**. The idea here is to quarantine your computer to stop the hacker from doing further damage.

2 CHANGE YOUR PASSWORDS EVERYWHERE!

Change all of your passwords. Start with your main email account, since all your password resets for all your other accounts will typically be sent to your email. Once that's done, reset the password for all your financial and other critical accounts. Now, I cannot stress this enough: **never reuse your passwords!** Also make sure that your new passwords are long, complex and unique to each account. Don't despair, Remote Desktop Manager can help you with that!

3 SET 2FA WHEREVER POSSIBLE

Turn on 2FA everywhere that you can to add an extra layer of security to your account. 2FA will use something you know, something you have, or something you are to properly authenticate you. I suggest you take a look at our review of the most popular 2FA tools.

4 UPDATE, SCAN AND (POSSIBLY) RE-IMAGE YOUR SYSTEM

You know that something bad is living inside your computer, and you need to get rid of it. Start by updating your software to ensure that you're running the latest version of your operating system, and download a reliable anti-virus. Once that's done, scan your system for any malware and viruses. If you really want to be on the safe side, you can re-image your computer, wipe the hard drive, and re-install the operating system and all your apps. If you aren't an IT pro, then this might be the ideal time to call your favorite geek and ask for help.

5 START SPREADING THE NEWS (PART 1)

When Frank Sinatra sang "start spreading the news," he was excited about heading to New York, New York. You also need to spread the news, but this is a lot less exciting. In other words: tell your family and friends about the attack because hackers like to use their victims' address books to launch spear phishing campaigns (these are when hackers use personal information to send emails, social media messages and texts that look like they're sent from someone who the victim knows and trusts).

6 START SPREADING THE NEWS (PART 2)

Once your contacts have been warned, it's time to report the attack to your bank. If you suspect identity theft or this has been confirmed because fraudulent information appears in your bank account or credit card statement, contact your local law enforcement and report it. It's also wise to file an initial fraud alert with credit unions (in the U.S., the big 3 are Equifax, Experian and TransUnion). Also, if you know where the attack originated (e.g. a website that hit you with drive-by download), then let them know so they can investigate and prevent other people from being victimized.

7 CHECK FOR BACKDOORS

Once you've done all of the above, you may feel that everything is back to normal. But is it? While all hackers aren't the geniuses that are portrayed in movies and on TV, they aren't stupid, either. Many of them install a backdoor, which allows them to regain access even after you've upgraded your system and cleaned up your computer. Don't take any chances! Verify your email rules to make sure that emails aren't getting forwarded to another account, and check your security questions to see if something suspicious is going on like questions that might have changed.

A Note About Ransomware

Ransomware is a massive problem these days. In fact, in 2017, ransomware attacks around the world jumped by 250%. If a hacker is demanding that you transfer hundreds or thousands of dollars in crypto currency or else you'll lose all of your files, what should you do?

Truly, there is no absolute right answer to this. Some experts advise against paying for a couple of reasons: 1) it gives hackers an incentive to keep extorting victims, and 2) there's no guarantee that even if you pay you'll get your data back. On the other hand, you may find yourself attacked again in the future because hackers know that you're willing to pay.

Ask Yourself Why

Once you've put this scary situation behind you, it's important to reflect on why you were hacked, and identify what you can do to minimize the chances of going through this again. We suggest using good password management software to create and securely store strong passwords. Together, we can make things a bit safer out on the virtual landscape.