

"Local Support • Personal Service • Since 1976"

www.ccstech.net

"Relax...we're on IT"

300 Main Street, Coopersville, MI 49404
616.997.TECH(8324)
Fax 616.997.9317

206 Washington, Grand Haven, MI 49417
616.842.TECH(8324)

3489 Kelly Street, Hudsonville, MI 49426
616.669.TECH(8324)



Was I Just Hacked?

by Ryan McMillen

Hello, I have bad news for you. I have hacked your e-mail account and there's nothing you can do about it. Your password is **654RTfg** right? Now pay me money.

You may have seen an e-mail like this floating around your inbox and it can be quite scary. Especially if it is a password you have used! What's this all about? It's a new spam campaign that is meant to create fear in the reader. The sender accuses you of doing something inappropriate and suggests that unless you pay him some bitcoin, he's going to let everyone know. This is most likely a complete bluff. Here's how it works.

The Dark Web is the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable. This is where experienced users go to purchase products and services that are, in many cases, illegal. Unless you or I run special encrypted browsers, we cannot visit sites on the Dark Web. One of the services that you can purchase here are username/password lists. People buy these lists with untraceable crypto currencies, then spam these e-mails with passwords that have been cracked in an attempt to extort money from these users. It's actually pretty ingenious and very scary.

How did they get my password? Well, remember when you heard in the news that there was a security breach at Home Depot? Or Sears, or K-Mart, or Delta, or Macy's, or Panera bread... you get the idea. You may have heard that users that entered their personal information on these sites "may" have had their data compromised? Well, that's how these passwords end up on the Dark Web! Now, if you use the same password on multiple sites, it is possible that the password and e-mail address that you used to make an online purchase at Home Depot is the same password and e-mail address you use to access your bank account. Nervous yet?

So, what can you do? Here's my first piece of advice. Change your passwords now if you have not done so in at least 6 months. By doing this, information on the Dark Web that has been sold will now instantly be incorrect. Second thing to do is invest in a good password manager and then make sure you protect THAT password manager with anything you can. Use a fingerprint, 2 factor authentication, etc. One of the best password managers over the last few years has been Dashlane. It helps keep all your passwords safe and even helps you create complex passwords that you don't even have to remember! Furthermore, it alerts you to hack attempts that affect your specific passwords, so you can get them changed immediately. The price of this service is anywhere from FREE to about \$10 a month depending on what you need. We have a link on our website to try this at ccstech.net/dashlane

Another tool we highly recommend, especially if you are a business, is our ID Agent service which runs \$99 a month for your entire organization. Using this service, we run reports on every employee on your domain (e-mail system) and determine if any of them have compromised passwords for sale on the Dark Web. Each of these compromised accounts present an immediate security threat to your business! Even users that no longer work there can make your life a nightmare if they still have some active accounts on your network. Furthermore, this service monitors Dark Web Activity and we immediately get in touch with you when an alert goes out. If one of your employees has their information exposed online or is for sale on the Dark Web, we can let you know asap so you can make sure the proper password changes have been made. You can give us a call or visit ccstech.net/id for more information. It's an incredible value for only \$99 /month and it just might help you avoid the costs or lost data associated with a major hack attempt!

So don't ignore news articles that announce security breaches at stores or websites you frequent. Instead, take action and get with a CCS Technologies technician! Let us show you best practices to protect and monitor yourself and your staff.

"Relax...we're on IT"

Contact Information

Information	info@ccstech.net
Tech Support	support@ccstech.net
Sales	sales@ccstech.net
Ryan McMillen	rmcmillen@ccstech.net
Greg Slater	gslater@ccstech.net
Ellen Slater	eslater@ccstech.net
Joe Halstead	jhalstead@ccstech.net
Jorge Arias	jarias@ccstech.net
Drew Rowe	drowe@ccstech.net
Jeff Verry	jverry@ccstech.net
Karen Strickland	kstrickland@ccstech.net
Nick Dykstra	ndykstra@ccstech.net
Eric Ruzek	eruzek@ccstech.net
Rich Raab	rraab@ccstech.net

CCS Technologies Store Hours

Coopersville Store

Mon-Thu 8 - 5:30 & Fri 10 - 5:30

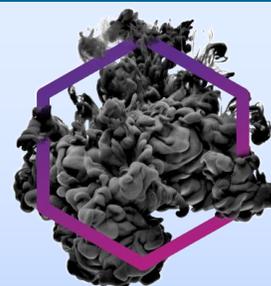
Grand Haven Store

Mon-Thu 9 - 6 & Fri 10 - 6

Sat 10 - 3

Hudsonville Store

Mon-Thu 9 - 5 & Fri 10- 5



DARK WEB ID

Bring to light emails and passwords that have been compromised and are for sale to the highest bidder, BEFORE a breach occurs.

We present data evidence that has been analyzed and validated, to deliver solid justification for added security measures, such as 2FA or employee security training.

Easy to deploy, Award Winning

Constantly monitors the Dark Web for a breach and alerts CCS Technologies immediately so we can work with you to enhance security for your company.

Covers your ENTIRE organization for only \$99 per month!