CCS Technologies

June 2018
Volume 13, Issue 6

"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)

Attention Office 365 users… Hackers are targeting you!

Here's how it works:
Hackers write automated programs that do nothing but guess random email and password combinations for common email services like MS Office, Apple, Gmail, Yahoo, etc. They can guess 350 billion combinations per second and work around the clock worldwide. ***Then…***

1. Your e-mail account gets "cracked" by the bot guessing your password.
2. It sends out an e-mail from you asking other people (as if it came from you personally) to sign in to their account so they can read a secure document "you" sent.
3. It creates a rule in your inbox so that if any of the people receiving your email responds, you never see the response.
4. It can now interact with people in your contacts. It can answer their questions like "Did you really send this?"
5. All of this goes on without your knowledge.
6. Now the program has your friend's credentials and can do the same thing with their account.

Think of the damage this can do! The unsuspecting recipient believes that you personally are requiring them to enter their credentials so they can see your "secure" correspondence. They are even communicating with these unsuspecting people without your knowledge and impersonating you and people are falling for it! The end result is a mess and can really put a strain on your business relationships.

This is happening more and more and we are being as proactive as we can to make sure this does not happen to you. **Here are our recommendations:**

1. **Outbound spam filtering!** For those of you who have our Office 365 services, we will be employing filters which will check outgoing mail, in addition to the incoming mail filters you already have, to make sure you are not sending spam without your knowledge. You may be hearing from us about this soon.
2. For those of you who do NOT have our Office 365 product, you may want to reach out to us and see if we can add our filtering service to your existing mail service.
3. For EVERYONE we suggest changing your password **immediately** if you have not done so in a while or if your password is not complex.

Passwords: Complexity does not necessarily mean "a bunch of random stuff."

Our current recommendations are as follows…

1. **Activate two factor authentication** if you have not done so already. This means that someone needs access to your username/password and one of your other physical devices to get into your account. This eliminates vulnerability to brute force attack from the outside.
2. 8 characters or longer. The longer the better!
3. At least one uppercase and one lowercase.
4. Try to avoid using words that are in the dictionary but if you must use them, separate them with numbers.
5. Add symbols but do not use a symbol to substitute as a letter (examples: @ for "a", or 1 for "l") This no longer works as the hackers already check for this.
6. Words or "non" words should not have anything to do with each other, your e-mail, your business, your name, etc. It should not be something anyone could guess or look up.

That's really all there is to it! See? It does not have to be overly complex, and by using words and numbers, you can easily remember them as opposed to remembering randomized letters and numbers (which is not significantly more secure than this suggested method) and you are less likely to forget it.

Here are some examples of BAD passwords:
Smith123 – It's barely long enough but it has your name in it. 123 is the least secure set of numbers to use in a password.
W@ypoint – This one is super easy to crack. Waypoint is a dictionary word. Hackers will use a dictionary program that knows which letters can be substituted for symbols
H$1df23 - Seems like a good one, right? At least it's hard to remember. Nope. Not long enough.

Here are some examples of GOOD passwords:
Gurl4345Maco – Girl and Mako have nothing to do with each other and are misspelled. Words are separated by an number which makes it more difficult to crack with dictionary tools. Caps are used.
Blak7621attaK! – Now we are rhyming and maybe using a 4 digit pin that you can remember
bRase#forEm – Separated non-words that actually sounds like a sentence. Brilliant!

So please change your passwords. If you are unsure whether or not your organization employs an outbound spam filter to catch stuff that might be sent without your knowledge (or your staff) just call us! We can check to see if you are protected. And if you are not, we can explain what needs to be done. Don't wait for this to happen to you. *CCS Technologies* has seen it and literally have had "conversations" with the hackers. It's creepy and is happening more and more. Let's get ahead of this latest threat before your clients, family members or anyone else is tricked… and now THEIR account is at risk!

"Relax...we're on IT"

Contact Information

Information	Info@ccstech.net
Tech Support	Support@ccstech.net
Sales	Sales@ccstech.net
Greg Slater	Gslater@ccstech.net
Ellen Slater	Eslater@ccstech.net
Drew Rowe	Drowe@ccstech.net
Jeff Verry	Jverry@ccstech.net
Joe Halstead	Jhalstead@ccstech.net
Jorge Arias	Jarias@ccstech.net
Karen Strickland	Kstrickland@ccstech.net
Mark Kowitz	Mkowitz@ccstech.net
Ryan McMillen	Rmcmillen@ccstech.net
Eric Ruzek	Eruzek@ccstech.net
Seth Johnson	Sjohnson@ccstech.net
Nick Dykstra	Ndykstra@ccstech.net

CCS Technologies Store Hours

Coopersville Store
Mon-Fri 8 - 5:30 & Sat 9:30 - 12:00

Grand Haven Store
Mon-Thu 9 - 6 & Fri 10 - 6
Sat 10 - 3

Hudsonville Store
Mon-Thu 9 - 6 & Fri 10- 6
Sat 10 – 1

Lenovo Tiny

Intel 2.70 Ghz Core i5 Quad-Core CPU
8GB DDR4 RAM
256 GB SSD Hard Drive
Intel HD Graphics 630
Integrated Sound & Bluetooth 4.1
Gigabit Ethernet & Intel Dual Band wireless AC
6 USB Ports & 3 DisplayPorts
USB Keyboard & Optical Mouse
Windows 10 Professional 64bit
12 Month Mfg. Warranty

~~SALE $999~~ SALE $899

Setup and Ready to Use!

Prices good through 6/30/2018

While supplies last