Cybercriminals Are Counting On You Letting Your Guard Down

The world is slowing down during this COVID-19 pandemic. Wall Street is being hit hard. People are no longer going out. We're told to quarantine or self-isolate and not engage in groups.

There is one group that's not slowing down at all: Cybercriminals. In fact, they're probably working overtime while the rest of us have our lives turned upside down. These cybercriminals and hackers know there's no better time to strike than during a global crisis. While you are distracted and spending your time trying to make sense of this new normal, they are finding new ways into your IT network so they can steal data and passwords, compromise the private information of your clients, and even demand large ransoms.

Cybercrime is already on the rise and is expected to cause $6 TRILLION in damages by 2021. Unfortunately, hackers may be out in full force throughout this coronavirus scare. In just a few weeks we may start seeing headlines change from stories about COVID-19 to accounts of cyber-attacks on corporations and small businesses.

Here are solutions you can implement now to help protect your business data, money and productivity:

1. **Be more suspicious of incoming e-mails**

Because people are scared and confused right now, it's the perfect time for hackers to send e-mails with dangerous malware and viruses. At this moment, your in-box is probably filled with "COVID-19" subject lines and coronavirus-focused e-mails. Always carefully inspect the e-mail and make sure you know the sender. There's a cdc-gov e-mail address out there now that's not legitimate and is spamming in-boxes across the country.

Avoid clicking links in the e-mail unless it's clear where they go. And you should never download an attachment unless you know who sent it and what it is. Communicate these safeguards to everyone on your team, especially if they are working from home.

2. **Ensure your work-from-home computers are secure**

Another reason we expect a rise in cyber-attacks during this pandemic is the dramatic increase in employees working from home. Far too many employers won't think about security as their team starts working at the kitchen table. That's a dangerous precedent.

First, make sure your employees are not using their home computers or devices when working. Second, ensure your work-at-home computers have a firewall that's turned on. Finally, your network and data are not truly secure unless your employees utilize a VPN (virtual private network). If you need help in arranging your new work-from-home environment, we would be happy to get your entire team set up.

3. **Improve your password strategy**

During crises like the one we are all facing right now, your passwords could mean the difference between spending your time relearning how to grow your business and trying to recoup finances and private data that’s been hacked. Make a point now to reevaluate your passwords and direct your team to create stronger passwords.

Also, while it’s so convenient to save your passwords in your web browser, it also lessens your security. Because web browsers simply require their own password or PIN to access saved passwords, a skilled hacker can bypass this hurdle. Once they access your saved passwords, they can steal as much as they want – credit card information, customers’ private data and more!

Instead, you should consider a password manager to keep all of your passwords in one place. These password managers feature robust security. A few options are LastPass, 1Password and Keeper Security Password Manager.

You, your team and your family have enough to concern yourselves with in regards to staying healthy, living a more isolated lifestyle and keeping your business strong. There’s no need to invite in more problems by letting your computer and network security slide during these times.

If you need additional security advice or would like to have a consultation to discuss how to keep your data safe, simply connect with us today.