How to Protect Your Data at Home

Devolutions

WE ALSO NEED TO PROTECT OUR PERSONAL ACCOUNTS AT HOME BECAUSE CYBER CRIMINALS ARE ALWAYS LOOKING FOR OPPORTUNITIES

We all know that protecting data at work is a critical priority, since **a breach can lead to customer loss, reputation damage, investigation and remediation costs, and possibly even lawsuits, fines and sanctions.**

As scary as this sounds, there are ways to reduce the risks of getting hacked, such as using a strong and reliable password management tool — and not a spreadsheet and sticky notes (AHHHHHHH!).

What are your personal risks?

But at the same time, we also need to protect our personal accounts at home — because cyber criminals are always looking for opportunities to target individuals, and not just businesses. No, if you get hacked it's not going to make the headlines, and your CEO isn't going to call you in for a terrifying meeting. But this doesn't mean you should let your guard down.

Unfortunately, hackers aren't interested in stealing Candy Crush credits. They're after one thing: **money**. And they're very good at hunting down sensitive data. For example, let's say you recently bought a new gadget, and stored your credit card information on the seller's website to save time and effort for a future purchase. A successful hack would put that information in the hands of cyber criminals who could **wreak all kinds of financial havoc, including identity theft**. And it gets even worse.

Hackers are like evil detectives. They follow clues (i.e. bits of data) to inflict maximum damage. For example, by stealing social media credentials they learn all sorts of things about their victims: where they live, where they work, where they go on vacation, who their friends are…and the list goes on. And they can piece all of this information together to build profiles, and launch spear phishing campaigns. And **don't underestimate how much personal data is out there on social media**: here's what Facebook knows about you.

Protecting your data at home

If you use Remote Desktop Manager (RDM) at work, then you may be able use it to store your personal passwords and accounts, instead of in your browser. Remember: **RDM licenses are per user and not per machine**, which means that you can install your license on your work computer as well as your home computer using the same license. You can create a private vault inside your organization database to store your personal data, which only you can access.

However, your company policy may not allow you to access RDM from home for personal use. If so, then you can **either buy your own licence, or you can simply download Remote Desktop Manager Free**. Voila. Problem solved!

You may also want to take a look at Devolutions Server (DVLS) which now offers a web application to manage all your passwords. Feel free to request a live demo with our specialists: https://server.devolutions.net/home/requestdemo

And of course, RDM and DVLS aren't the only password managers available. There are many that you can choose from, including these popular tools.

More advice

Here is some other advice to help keep you safe at home:

- Avoid these 5 password security mistakes
- Use these 6 tips for safer online shopping
- Never save passwords your browser
- Use 2FA or MFA
- Use a credible antivirus (free or paid) and firewall.

Additional tips

If you have any additional tips for our community, please share them. Your experience and insight could **save others from a costly and stressful nightmare.**