6 Cybersecurity Mistakes a Freelancer Can Make - How to Avoid Them

Cybercrime has always been an issue ever since digital technology became a necessity in our daily lives. According to a Cybersecurity Ventures report, approximately 500 million personal records were stolen by hackers in 2018. The statement added that the finding is a 126% jump compared to a similar study in 2017, which is alarming.

These cyberattacks target all kinds of people and organizations, including freelancers. As a matter of fact, freelancers like you are among the primary prey of cybercriminals. But, you can apply simple countermeasures to protect yourself from cyberattacks. What are they? Well, it's by avoiding the six cybersecurity mistakes that you might make or have made in your freelancing activities. We're going to discuss each of them in this blog.

Not Installing Free Antivirus Software

Many freelancers give free antivirus software a pass because they think they aren't effective enough. Well, they're not as strong as expensive antivirus software, but they do provide basic protection. Free antivirus software protects you from phishing, accidentally downloading suspicious data and malware, and other common cyber threats. They automatically notify you if questionable elements have entered your computer.

Free antivirus programs are like free vaccines that protect children from harmful diseases. They're offered for free for a good reason. Think of your computer as your child. If you don't vaccinate your child, his or her health is at risk. So, make sure to install a free antivirus program on your computer. Choose one that is developed by credible and legitimate software developers. Some ads on the internet offer free antivirus, but they come from hackers, so make sure to avoid them. But, if you can afford to install a premium antivirus program, that would be much better.

Not Setting Strong Passwords

Of course, setting passwords is a security measure that all of us apply, not just freelancers should follow. But a common mistake most people make is setting weak passwords. Examples of these are common words with few characters and passwords that have a direct relation to a person. Hackers can guess or crack such passwords with ease, especially if they have specialized hacking tools and software at their disposal. So if your email account, social media accounts, online bank accounts, and files' encryption have weak passwords, you're making things a lot easier for hackers.

If you think your passwords are weak, start changing them now. Set passwords that have no connection to you. Entirely random passwords consisting of multiple characters are the strongest. Yes, password managers can help, but they have some history of being hacked. So, it's probably best to set passwords on your own. In setting passwords, you can type at random and take note of what you've typed. In that way, you can set passwords that have zero personal connection with you.

Passwords such as these would be ideal: "gios vosamfig 415," "352tgfdsgar23tys," "fdifjqvjgwofhqn3592y." As you can see, those types of passwords aren't even words anymore. They're more codes with absolutely no definition.

Not Using a VPN

As a freelancer, it's a given that you communicate and exchange important data with your clients online. The data that you share to and receive from your clients could be in grave danger if you're not using a virtual private network or VPN. Data that are transmitted without a VPN is like throwing goods into a nest of vipers. Once hackers intercept your data, it's not just your security that's affected, but also that of your clients. In that case, your online reputation as a freelancer will degrade immensely. You could lose your clients, and ultimately, your career as a freelancer could end.

Whatever sort of freelance work you do, spare some money from your income to use a VPN. VPNs provide you with a secure online browsing experience. They act as a strong protective barrier against common malware and scams online. See to it to choose a VPN that has updated encryption methods. Why? That's because hackers develop new techniques to breach VPNs. If you use a VPN with an out-of-date encryption setting, your computer is still at risk.

Indeed, using a VPN will cost you more money. But think about it; you could lose even more assets if you expose your online activities.

Not Assessing the Security of Public WiFi

If you're a freelancer who prefers to work in coffee shops and public libraries, be careful of using these establishments' WiFi connections. You might assume that they're safe because reputable establishments own them. But in reality, public WiFi connections are cybercriminals' favorite hunting grounds. Some of these cybercriminals create fake WiFi hotspots with the establishment's name on it. For example, if a coffee shop's name is "Blue Fudge Cafe," the phony WiFi hotspot's name could be "BlueFudge_WiFi." If you immediately connect to a public WiFi without checking whether it's credible, your cybersecurity will be in jeopardy.

So before you use a public WiFi, make sure to consult an establishment's personnel first. Ask them if the WiFi hotspot your device detected is theirs. But, the best counteraction is never to use public WiFi in doing your freelance work. It's more advisable to have your WiFi connection at home for better data protection.

Not Being Wary of Physical Surroundings

Even if you have topnotch security software, VPN, and strong passwords, your cybersecurity could end up in hot water if you're unwary of your surroundings. If you usually work in a public place, know that some cybercriminals do their activities without using digital tools and gadgets. If they see an opening, they'll glance at your computer screen or keyboard strokes to get private information. That's all it takes for them to hack you.

So always be wary of your physical surroundings working in public areas. Make sure there's no angle for anyone to see your computer screen and your keyboard strokes. If you're bringing USBs with confidential files, don't just leave them on the table. Keep it inside your bag if you're not using them yet.

But, in our opinion, the best place for you to work is at your home. At home, you don't need to worry about your physical surroundings. Plus, you can probably focus because it's your private space, and you can boost your productivity.

Not Backing Up Important Files

The worst-case scenario is losing your files because of hackers. Of course, you don't want that to happen, but it's essential to expect the worst and have a contingency. If you don't back up your files, you'll have nothing to begin your recovery if the worst happens.

So as a contingency, make sure to back up your freelance portfolio, contract documents, client data files, and other essential information. Save other copies of your data on separate drives or upload them using cloud software or tools. Don't just have two copies of each file. Produce as many copies of them as you can just to be sure.

As a freelancer, practicing effective cybersecurity measures should always be a part of your basic operations. If you have made some of these cybersecurity mistakes before, make sure to avoid them next time. Always observe proper cybersecurity measures to nurture the growth and stability of your freelance business.