How Freelancers Can Ensure Client Data Is Protected

An analysis report from Verizon indicates that 43% of cyberattacks target small businesses. And, 60% of these small businesses hit by cyberattacks close within six months, according to Inc. Freelancing can be considered as a small business. It's a small business with only one worker, and that is the freelancer itself. In that case, freelancers are quite vulnerable to cyberattacks if they commit cybersecurity mistakes.

If you want to become a freelancer, among your checklist of obligations will be to protect your clients' data. Every bit of information your clients will share and disclose to you should be kept private and secure. Cyberattacks are your adversary in such matters. Here are eight cybersecurity measures you can adopt to ensure your clients' data will be protected.

Update Your OS Regularly

One of the characteristics of most operating system (OS) developers is to update current versions to new versions constantly. Sometimes it annoys us to the point when we don't really care if they announce updates. They seem unimportant and just a ploy by the developers to keep their OS products relevant. But in actuality, these updates can patch the security flaws of your OS's current version. When OS developers discover new forms of cyber threats, they formulate new components for the OS to block them. So, make sure to update your computer's OS regularly if you have the time. You can also switch on the auto-update option of your computer.

Install a Firewall

Each computer is preloaded with its own firewall. Firewalls function as roadblocks for hackers and malware attempting to breach a computer's systems. However, preloaded firewalls aren't flexible enough to fully prevent cyberattacks. For that reason, you should make room in your budget to install a third-party firewall. Third-party firewalls have more advanced qualities than preloaded firewalls. They have multiple layers of security that immediately hold cyberattacks from breaching.

You should also remember that malware can also originate from a questionable website you might accidentally open. If that happens, your third-party firewall app will block malware right away, and you'll receive notifications of it.

Set Strong Passwords

Most of us possess excellent skills in setting strong passwords for our social media accounts, right? Well, you should put those skills to good use in setting passwords for the systems holding your clients' data. Hackers can easily compromise accounts with weak passwords. Examples of weak passwords are those that have a direct personal connection with you. Your name, your birth date, and your pet's name are prime examples of weak passwords, and you should never use them. Your passwords must have at least 12 or more random characters, including numbers. If you see this as more work on your behalf, you can use a password management service.

Use Encryption

Encryption is critical to protect highly confidential data and information from your clients. If ever your clients' data is hacked or breached, their contents are still protected because of the encryption. Encryption is a set of random characters and symbols that distorts the actual contents of a document. Only authorized people can unlock it. In this case, the authorized people are you and your clients.

We assume that your primary communication method with your clients is through email. Keep in mind that emails can be susceptible to being intercepted by cybercriminals. So whenever you and your clients send and receive data to and from each other through email, make sure each of them is encrypted. You don't need to spend more money on encryption. There are free encryption services available such as ProtonMail and TrueCrypt.

Back Up Your Clients' Data

Backing up computer files is a basic method in securing data if ever they get corrupted, or we accidentally delete them. However, it's a method that we tend to overlook for some reason. But when it comes to securing your clients' data, you should definitely practice backing them up. You can create another copy of the data in another storage or save them online, such as in Google Drive.

You don't want your clients to get furious because you accidentally lost the important files they sent you. If that occurs, you might never receive a proposal to work for them again. Moreover, you should also back up your essential personal files, such as your freelance resume and portfolio.

Use a VPN

Your freelance job might incline you to research the internet every time, especially if you're a freelance content writer. But, in general, almost every freelance job requires an internet connection. That being said, it's best to integrate a virtual private network (VPN) program into your computer. VPNs cover up your IP address and your online browsing activities, making it hard for hackers to trace whatever data you receive and send to and from your PC.

Be Careful of Public WiFi

One of the amazing freelancer benefits is that you can freelance at home, which is a very comfortable place to work. You can also work anywhere you want, such as at coffee shops, cafes, and diners, as long as they have a WiFi connection. But, you should be careful of public WiFi connections. People using public WiFi connections are the primary targets of cybercriminals. Some of these cybercriminals set up fake WiFi connections with similar names with the public WiFi using their hotspot. If you connect to these fake connections, your computer and its files are at extreme risk. So, before you connect to a public WiFi, make sure to verify it first.

Use a Safe Payment System

When a client is on the brink of hiring you, they might ask you how you would like to receive your payment online. If your answer is through Paypal or Square, then the client will feel confident sending money to you. Paypal and Square are outsourced processors of online payments and transactions that follow the Payment Card Industry Data Security Standards (PCI DSS). The payments your clients will send you will be secure and protected. Paypal and Square are good examples of safe payment systems.

Among many practices, time management is often stressed as a crucial practice in being a freelancer. But, observing standard cybersecurity measures should also be emphasized, in our opinion. No matter how many sites for freelance work you'll visit, it'll be tough to earn the trust of prospective clients if your security practices are suboptimal. When you become a full-fledged freelancer, always make it a priority to protect your clients' data.