How Freelancers Can Protect Their Identity - 8 Ways

Freelancers like you must have a strong online reputation and presence to earn freelance work and have a steady income. After all, most clients and employers from big companies are primarily using the internet to search for available workers. The bottom line is that freelancers need the internet to run their business. Unfortunately, the web is full of cybercriminals with intentions to steal your identity. An analysis report from the 2019 Identity Fraud Study found that 14.4 million Americans were hit by identity theft in 2018. And according to various articles, cybercriminals are mainly targeting small businesses.

Keep in mind that your freelance business is a small business as well. That said, you could be vulnerable to identity thefts and other forms of cybercrime. Fortunately, there are practical ways to protect your identity, and we're going to break down eight of them for your benefit.

Be Careful of Public WiFi

Many freelancers prefer working at coffee shops and public libraries with free WiFi. If you're one of them, then you're saving a lot of money from monthly internet connection bills. But be wary. Areas with public WiFi are where most cybercriminals catch unknowing victims. They create their own WiFi hotspot with a similar name with the real WiFi connection of a particular area. If you mistakenly connect your laptop or mobile device to these WiFi hotspots, your passwords and other sensitive information are in jeopardy.

Kevin Coleman, the National Cyber Security Alliance executive director, says that people should avoid browsing through public WiFi connections. So, having your own internet connection or personal hotspot from your phone is the best option. It'll cost you more money, but it's better to be safe than sorry. You could lose even more money if your identity is out there in the open.

Reinforce Your Computer's Security

As a freelancer, installing anti-malware software and firewall into your computer is a must. It's one of the essential tips for freelance businesses.

Even though you avoid public WiFi connections, cybercriminals have other methods to steal your identity. Most of them will try to attack your computer system directly, which puts your identity and important data on a nest of vipers. For that reason, you have to reinforce the security systems of your computer. Anti-malware software and firewall can block suspicious elements from entering your computer, and you'll receive a notification should it happen. In that case, you'll be aware of threats that tried to breach your digital privacy. So make it a part of your budget plan to install security programs for your computer.

Protect Your Personal Info When Sending via Email

Usually, you send emails to your connections as a freelancer almost every day of your schedule, and they typically contain personal info. It's actually advisable not to transmit any sensitive data through your email, but circumstances require you to do so. So, the best counteraction is to protect any personal info using strong passwords. Any file attachments you'll send through email should require a code to unlock. Only you must know that code and the authorized recipient of your email. In this way, hackers attempting to intercept your sent emails will not be able to access the private info and data attached to them.

Use Two-Step Verification

Aside from passwords, a two-step verification security measure is another excellent method to protect your identity. It works like this, the recipients of your email will have to answer two questions that prove they are who they claim to be. So, if, unfortunately, a hacker succeeded in intercepting your email, at least he or she won't be able to access the data your email contains. The hacker doesn't know the correct responses to be granted access to the data. Only you and the authorized recipient can access it. Two-step verification tools are your data privacy's last line of defense. Files and data such as bills, quotations, invoices, receipts, bank account numbers, and social security numbers need to be protected by a two-step verification measure.

Don't Post Your Profile on Questionable Sites

It's common knowledge that freelancers like you find freelance work, attract clients, obtain referrals, and ultimately earn income through job sites and freelance websites. Those are online platforms where employers and clients post job opportunities. One of the benefits of freelancer jobs is that getting more work is quite convenient, thanks to freelance platforms.

But be wary of questionable sites that allegedly offer freelance gigs. We understand that you may be trying to boost the promotion of your service on multiple platforms, but you need to assess the credibility of a site first. Never post your profile and portfolio on questionable freelance sites. The operators of such sites might be hackers whose targets are job applicants. Instead, market your freelance service on reputable websites such as Upwork, Fiverr, Flexjobs, and Freelancer.com.

Background Check Every Client You Meet Online

Sometimes, you might receive a proposal via email from someone interested in hiring you. Of course, that delights knowing that a prospective client is considering you to work for him or her, but don't get too excited just yet. We never know if that person is really an interested client. Don't shrug off the chance that a person could be a cybercriminal who's been tracking you for a while.

Make it a practice to do a background check of each client you meet online. Ask their name, location address, and company or organization. Let them present a soft copy or a photo of their ID. Never negotiate terms and sign contracts with a suspicious individual. You need to take trusted clients only for the security of your freelance business and your identity.

Watch Out for Phishing

Phishing is a common cyber threat that everyone should look out, not just freelancers. It's a method cyber criminals use by sending emails or SMS with a message of greeting. Usually, the message is a congratulation that you've won some sort of prize or a high estimate of money. Phishing messages might also claim that credible companies sent them, but actually, they're not. If you click on the link contained within the message, you're putting your data privacy in danger.

You can identify phishing emails by their contents. If the message the email contains sounds generic and shows you a link with random characters, that's a good indicator that the message is a phishing attempt.

Get a Cyber Insurance

Despite the long checklist of precautions that you'll apply, still, you have to prepare for the worst-case scenario. For that reason, you need to consider investing in cyber insurance. Admittedly, it'll cost you and could hinder you from your goal to increase your income, but it's worth it to have a contingency plan if all else fails. Having cyber insurance will cover the damages and losses brought by a cybercrime. Subsequently, you can recover within a short period and put your productivity back to its usual rate.

Keep in mind that your personal files and information is money for simple hackers and people on the dark web. Don't let them profit from your lack of security measures. Safeguard and build a fortress around your data privacy at all times.