Your personally identifiable information may be at risk!

in most places where we provide our personal information, our PII is not remotely safe in any way, shape, or form. According to figures recently released, the U.S. Federal Trade Commission (FTC) received more than 5.88 million fraud reports in 2021.

Santa Ana, California Jan 11, 2023 (Issuewire.com**)** - We live in a world that has become almost completely dominated by technology, and we have become accustomed to using it in all aspects of our lives, both at home and at work. However, there is currently a hugely significant tech issue that no one is talking about, and it's related to our personally identifiable information (PII). "The bottom line is that, in most places where we provide our personal information, our PII is not remotely safe in any way, shape or form." Says Alvand K the CEO of intSignal.

According to figures recently released, the U.S. Federal Trade Commission (FTC) received more than 5.88 million fraud reports in 2021, a 19% increase from the year prior. Reports of associated financial losses topped $6.1 billion, which is an increase of more than 77% compared with 2020. These figures are astronomical, and not enough is being done to rectify the problems.

Many offices and businesses simply don't have the correct protections in place. For example, let's look at a standard dental or doctor's office. Most of these offices don't know the basic ePHI protection requirements, which is due to the fact that they are not being trained in the technology. Furthermore, if they were to hire an expert the costs would be incredibly high, which is simply not feasible for such small businesses. As a result, they often hire students, or someone with only limited technical knowledge to set up their printers and basic IT needs. In fact, the employees in most "tech support" companies are not trained to a very high level and often are only trained to carry out regular, tier 1-2 support tasks.

Based on our findings, most offices are using basic antivirus and backup solutions for their 'security', which is simply not sufficient. Furthermore, a large number are also employing legacy operating systems, such as Windows 7, that have now been discontinued, along with very weak security solutions, most of which have been breached at least once. These data breaches, often involving ransomware, involved an average of 1200+ ePHIs each time. On asking how these breaches had been addressed and remedied, we were told that they had restored the system from their backup and installed new antivirus software. That was it.

The failings in these systems can't be blamed on the doctors, dentists or business owners. The problems stem from a lack of awareness about the level and type of protection required, along with the need to have affordable access to experts, support and consulting services. Moreover, this is not just about doctors' offices, as this is only an example; it impacts most other businesses as well, even those within the tech industry.

Without promoting any particular company or product, we would suggest that good basic protection begins with the following:

- Disk encryption
- A good, premium antivirus software
- Reputable email servers that are compliant with today's standards
- Regular updates and compliant operating systems
- Reputable password managers

We would also advocate the use of an encrypted storage system with cloud backups and, preferably,

cloud storage sync that can be accessed securely over the cloud, and which also has backup retention.

To minimize interruptions, it is helpful to have all of the updates happening outside your normal operational hours, and ensure that everything is saved on separate storage devices, and not on individual computers. In addition, it is advisable to always have an extra computer designated as a backup, which can be used daily, just in case one fails. Finally, get into the habit of using secure passwords, and always use multi-factor authentications (MFAs) - preferably not ones sent via email, but through apps or text messages instead.

If you follow these low-cost tips, along with your local and national regulations, you can properly protect your patients' ePHI, as well as your business.

Media Contact

intSignal

publicinfo@intsignal.com

888-984-1634

Source : intSignal