

The Cyber Canary Is Announcing How It's Anti-Malware Helps You Fight The Three Biggest Online Threats To Your Computer In 2021.

The Cyber Canary is protecting people's devices against harmful malware that typically gets overlooked by big-name competitors.

The Cyber Canary has announced an Anti-Malware solution that is due to disrupt the antivirus industry. The Cyber Canary prides itself on the fact that its anti-malware protects users against online threats that free & other big-name competitors often overlook.

The number of cyber-attacks have increased by 300% in 2020 (FBI report). Exemplifying to all internet users that there has never been a more critical time to get protected. Here are the top three cyber threats that The Cyber Canary protects you against that you need to look out for in 2021.

Phishing Attacks Phishing attacks consist of a message sent to trick people into clicking on a link that can then expose them to malware and compromise their data. This message can take different forms such as emails, site downloads, or even email attachments from trusted sources.

With time these phishing attacks get more and more sophisticated. Hackers are getting even more creative in the ways that attack and compromise a user's computer. Therefore, it is vital to have a forward-thinking cybersecurity solution to protect your online information.

It is difficult to differentiate a phishing attack from regular emails. Suppose the user inadvertently runs the malware. Often, there is nothing to draw a user's attention to the malware executing, and the first time they realise there is an issue, it is too late. In that case, The Cyber Canary anti-malware feature detects and prevents any infection or suspicious activity by alerting the user and terminating the offending process.

Ransomware Ransomware consists of blackmailing the victim by hijacking information and holding it for ransom. Hackers use this method by encrypting users' files and then only releasing them if the ransom is paid. Often, even if the ransom is paid, the keys required to decrypt the user's files are never recovered.

In 2020, ransomware attacks cost victims 200 billion dollars. Many people who fall into ransomware traps are helpless with no choice but to pay the ransom. Otherwise, they risk losing personal files that the attacker has encrypted.

Ransomware is a severe issue ruining millions of people's lives around the world. Everyone should take it seriously and protect their sensitive and personal information.

Protect yourself from ransomware by starting The Cyber Canary limited time: 30 Day Free Trial.

Advanced persistent threats Advanced persistent threats (APT's) are malicious actors that gain unauthorised access to a system network or server and remain undetected for an extended period. During this time, important and often sensitive information is copied from the target back to a location controlled by this attacker. These types of attacks are targeted towards particular businesses & their employees.

Knowing that someone is roaming on your system can be challenging to detect, and many times are not noticed for many months, and in some rare instances, years.

Catching ransomware in action The art of detecting and protecting a user from ransomware can be quite tricky. A typical Windows 10 system has many hundreds of processes running at a given time, and each of these can be doing many things to files on your system. In a clean system, these are "friendly" processes and pose no threat. However, on a compromised machine, a lonely process can cause havoc and can destroy files in seconds. Determining the good from the bad is more complicated than it may appear. Typically, antivirus software tries to catch these destructive processes using signatures-based detection and heuristics. The result is that rogue applications can go unchecked and infect your device.

A more robust way of catching ransomware in action is to monitor the very files the ransomware is going to attack. That said, this is also tricky because it may not be possible to determine if the file was intended to be modified or not. The Cyber Canary unique approach takes aspects of file monitoring but mixes in our proprietary "canary" file technology. A canary file is a virtual file that only exists while The Cyber Canary is active. These files are used to monitor read and write operations by individual processes and determine if a malicious process is at work.

In addition to monitoring ransomware, The Cyber Canary can use these canary files to monitor system intrusion events by watching the read operations on canary files.

GET PROTECTED

Fortunately, we are not helpless in the fight against cyberattacks. Though, by using big-name anti-malware, you may not be entirely protected. With The Cyber Canary, a one-click Australian solution, you can get instant ransomware protection in seconds.

We now have a 30-day FREE trial offer so you can test our brand new software.

For business inquiries please contact:

Anthony Smith: anthony.smith@division-m.com

Related Links:

[Main Site & Plans](#)

[30 Day Free Trial](#)

Contacts

Anthony Smith

2392905361

[mailto: anthony.smith@division-m.com](mailto:anthony.smith@division-m.com)