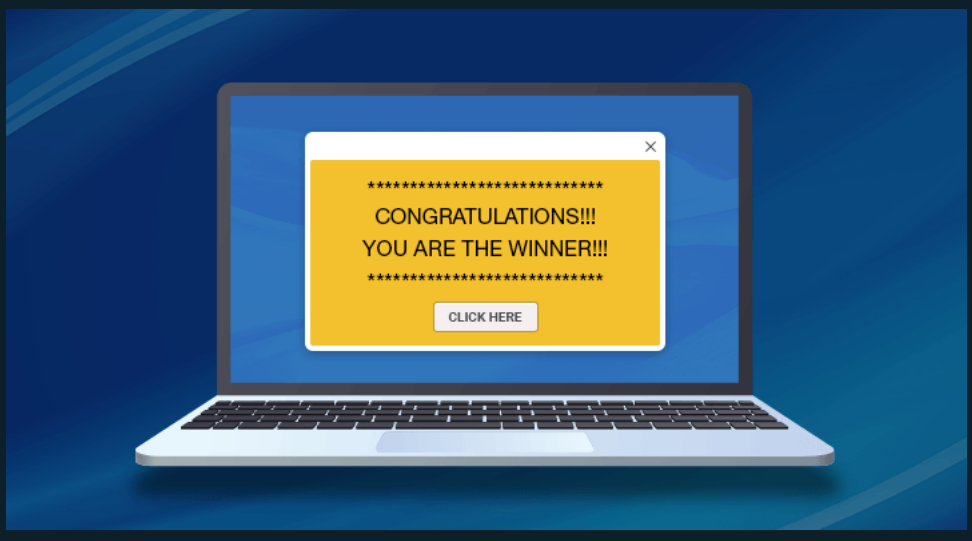
What is a Hacker (part 3): How to protect yourself

In today's world information has become our most valuable commodity, it's also our most vulnerable. Everyday when you are using the Internet, information about you and your habits is constantly collected and sold to the highest bidder. And what's worse; you are giving it to them for free and in many cases without consent. In the best of cases the only ones spying on you are advertisers, in most cases you have no idea, they might be hackers or they might be state-sponsored actors.

Steps to protect yourself

Following a few preventive steps, you can greatly increase your online privacy, protection and keep hackers away.



- **Update your devices**
  Updating all your Microsoft products is very important; enable automatic updates on both Windows and the Office Suite. Using old software is often dangerous since they have lots of unpatched vulnerabilities hackers can exploit.

- **Antivirus and anti-malware**
  If you are using Windows 10, you don't need antivirus since the system has one built-in, and it's one of the best. If you are using older Windows systems you should consider upgrading since the older systems have known vulnerabilities. Complementing antivirus; using anti-malware software is recommended, they might find threats Windows does not.

- **Don't use public WiFi**
  Public hotspots are a haven for hackers stealing data; they can be infected with key-loggers that steal all your login details or malware that infects your device. Even the password-protected WiFi on a hotel can be dangerous, you have no way of knowing it's the real WiFi or a hackers cloned WiFi.

- **Secure your router**
  Your Router is the first line of defense in your network; it's also a juicy target for a hacker since all information within a network passes through it. Ensure you changed your admin password from the default and use strong passwords for your WiFi-networks. It's also important to restart your router from time to time if a hacker as planted malware it's usually removed on restart.

- **Stop the tracking**
  Data has surpassed oil as the world's most valuable resource, and that resource is being gathered for free at the expense of your privacy. Whenever you are using the Internet, advertisers track what sited you visit and deliver targeted advertising to you. Hackers use the same tools, masquerading as advertisers, collecting information and delivering malware through ads. Using an trusted adblocker plugin for your browser is a good way to stop the tracking and reclaim ownership of your data.

- **Use strong password**
  Passwords comprised of multiple words combined, i.e. "appleorangekiwi" are easily cracked using simple dictionary attacks. A good password combines letters and numbers and unique non-dictionary words, i.e. "applezOrangezKiwwwiz47" would be much harder to crack. It's advised never to use the same password on multiple services, if remembering all those different passwords seems hard, use a password manager.

- **Enable 2FA (two-step) authentication**
  Whenever you can use 2FA you should, it's an extra layer of protection against hackers. The first step is your normal password, and the second (2FA) is usually a pin-code you have to enter, sent via SMS or email.

- **Use VPN**
  Using a Virtual Private Network (VPN) encrypts your internet connection and makes you anonymous online; this protects your personal information. It also has the benefit of stopping a lot of advertisements and tracking of your information.

- **Think before you click**
  Many infections originate from phishing emails or websites; they are designed to look legitimate but contain malware infecting the user. As a rule of thumb, don't click links in emails or download attachments, always google the name of the company to check if the information is legitimate before doing anything else. If you get an email from a known sender that only contains a link without any text, the sender's account could be hacked.

BitIDentify

Bitidentify SDL proactive security

Bitidentify uses Proactive Security rather than reactive; we built our system around never having your data connected to the internet. If a hacker can't see your data, it can't be stolen or even targeted for attempted hacking.

The core of our system is a bare-bones Linux OS (Host) that uses virtualization technology to run two instances of Windows (Guests) on top of it. The Guests are the Open and Secure Machines:

- **Open Machine** is connected to the internet like a normal PC.
- **Secure Machine** is isolated from the internet and used for classified information only.

The user works with confidential data on the Secure Machine and switches to the Open Machine when there is need for internet. By using virtualization technolog, we can offer features normally not available on a standard computers:

- Ability to completely remove any virus or malware with our unique Restore-function.
- Ability to access-control all USB-devices connected to the computer.
- Running Windows OS with the security of the Linux OS.

Original post can be found at our homepage:
https://www.bitidentify.com/blog/hacker-how-to-protect-yourself/