Guide

Gearing up for safe remote work

Paweł Wałuszko 27.03.2020

Given the current COVID-19 pandemic, many people are considering working from home. Some of them will probably take home a business laptop, which has been prepared by the IT Department. From a cybersecurity standpoint, this is the best option: the employee takes home a ready-to-use device, with all software pre-configured and a VPN client to connect to the business environment. In such a situation, all security measures are already taken care of by the employer, and all the employee has to do, is to plug the machine into a home network and get online.

The other option is to utilize a personal computer in order to work remotely. As much as it seems quite easy to get up and running – as it's only a VPN connection away – it's a good idea to get yourself properly set up before your computer ends up being the one which infects others at the office.

The basics

Always try to separate business and private environments.

The best way to achieve this, of course, is by using a separate computer for business and private use.

Separate devices support privacy

First, utilizing such setup will save you from various privacy-oriented mishaps, such as accidentally attaching a personal document to an email, having private messages show up in the middle of a presentation, or your browser history popping up at the least fortunate time – such as during a webinar. Even if you remove your browsing history, the *autocomplete* as well as *Open Recent Documents* functions show up in various programs and can be quite revealing. Operating systems are designed to be automated and ergonomic, so a list of recently opened pictures or contents showing up at the most unexpected moment – in theory, to make your life easier – can expose a lot of private information.

Second, keeping private software off company records is in your best interest. A typical home computer is littered with various software downloaded from numerous sources all over the Internet. Some software may be legitimate. Other software, however, may appear to be functional, however, in the background it may contain a malicious function – such as keylogging, taking screenshots or allowing remote control. In fact, this is a common way for hackers to spread malware. When typing a corporate password on a personal computer, unknowingly, you may be transferring this password to cybercriminals. Moreover, ransomware, which has wreaked havoc in government and in business sectors, can stay dormant until it detects a certain environment – such as a Windows Server machine. In the meantime, ransomware can quietly stay on your computer, slowly encrypting files, or waiting for a good moment to reproduce.

Last, but not least, there's the software licensing issue. While installing software (or even turning on the computer for the first time), the user is presented with lengthy software license agreements (often abbreviated *EULA*) for nearly all pieces of software. Most users have probably never read the agreement – and that's the problem. A sizable amount of free-to-use software is only free for personal or educational use. Utilizing the same software for business often constitutes a break of the license agreement and can have various repercussions: from legal action by the vendor to having the license suspended. This brings us to the second point:

Don't cut corners. Invest in legitimate software.

There are countless sites out there that host copies of pirated business software – such as Microsoft Office. Moreover, they usually have a license key attached, ready to be activated. Given that a fresh copy of Microsoft Office can cost a few hundred USD, this may seem like a great way to save money.

Not necessarily so. When downloading software from unverified channels, the user has absolutely no guarantee of what the software really contains. The file user thinks is Microsoft Office may flat-out be a virus. Even if the file is indeed a Microsoft Office installer, there's no guarantee what other types of code the installer is laced with. The user might end up with a working version of the said Office suite, plus a few pieces of malware to go along with that.

Utilizing online-found license keys for paid software is also not a good idea. As most paid software today is activated online, it's apparent to the vendor who is legitimately activating their product. During the activation, the computer contacts the vendor's servers send a copy of the license key used to activate the software, as well as additional supporting information. This supporting information can be your environment information (such as operating system version), user information (entered during the setup process or during Windows installation process) and your IP address, which can be used to track down your location. In the best-case scenario, if the vendor is suspicious, they might not activate the product. In the worst-case scenario, the vendor can take legal action against the user for alleged software piracy.

Then there are the updates. Most software, when not properly registered and activated, loses the ability to download updates, which in many occasions defeats the point of having such software to begin with. A great example of this is antivirus software, which relies on daily updates of virus definition files. As the definition file lets the software know how to define a virus and what to look for, having an outdated definition file renders the software nearly useless.

Of course, there is a legal way around this situation: utilizing open-source software. As open-source software is free to use in a personal and business environment, it's worth taking a look at open-source alternatives to common commercial programs. This list provides a good starting point.

Building up your security

Since most computers sold around the world are pre-loaded with one of the versions of Windows 10 (Home, Education, Pro or Enterprise), let's focus on Windows 10 basic *security hardening* and good practices for safe Internet usage.

If you're already set up with a computer and legitimate, functioning software, here are some steps to make your remote work more secure:

Regularly update your software to the latest version

If your software has an auto-update function, enable it. If your software requires manual updates (such as drivers), periodically check in on the vendor website for possible updates. Keep in mind that software updates do not necessarily bring in new features, and in fact, sometimes visually, absolutely nothing will change. However, updates often address performance and security issues, which are strictly under the hood.

Create a separate, underprivileged account for everyday use

Upon installing, Windows 10 automatically creates a user for the computer. By default, this user can install software and change certain security settings. In theory, this is a good idea, as the user can customize and install software to his desire. However, from a security standpoint, it's always best to utilize the *least privilege principle*: if you don't need to use the computer as the Administrator, run as the least-privileged user account. By utilizing an underprivileged user account for everyday use you guard your computer against accidentally installing software that might pop up on your screen.

Always use two-factor authentication, whenever available

With time, software vendors and service providers realized that password protection is not a sufficient method of protecting data. Computers can be hacked, they may contain malware and can be physically stolen. A password entered on a compromised computer offers virtually no data protection. As such, the industry has been moving to utilize two ways to authenticate a user. Most commonly, it's done with the help of a second device, such a smartphone. The idea is simple: it's much more difficult to steal or hack into two separate machines at once, so a confirmation of a login – such as by receiving a text message with a unique code to type in – offers a much improved way of verifying the true identity of a user.

Conduct an audit of your installed software and turn off unnecessary services

Just like smartphone manufacturers, computer hardware manufacturers sometimes pre-load their computers with a certain trial or freeware programs. It's a good idea to verify what each piece of software does, what's its function and whether or not it sends any data to the Internet (such as a cloud backup service). Additionally, turning off certain services, such as *Remote Desktop*, if not used, is advisable.

If you're working on a laptop, encrypt your hard drive

The unfortunate thing about mobile systems is the fact, that they can be easily stolen. This is why in Windows 10, Microsoft introduced hard drive encryption into every version of the operating system. Windows 10 Pro, Education and Enterprise can utilize BitLocker. Users with Windows 10 Home can utilize the Device Encryption utility, as long as their hardware meets Microsoft's guidelines. Step-by-step instructions can be found here.

To sum up

Windows 10 is a significant step-up in terms of Windows operating systems security. In comparison to some of the previous versions, it comes with a built-in firewall, antivirus program, and hard drive encryption features, which used to be added manually in previous versions. Out of the box, it's a fairly safe system, and as long as we utilize best practice security advice, it can be safely used to work remotely. Regardless of its relative security, however, it's best practice to keep the business and private environments as separate as they possibly can be, and that would be my number one advice to anyone considering working remotely.

Rate the article:

★★★★★ 5 / 5 (2 votes)

27.03.2020

Paweł Wałuszko

Business Development Manager i Ekspert ds. Bezpieczeństwa. Doświadczony menedżer w branży IT, który swoje doświadczenie zdobywał m.in. w Dolinie Krzemowej; entuzjasta oprogramowania open - source.

How CEOs fall victim to hackers. The example of Jeff Bezos

Remote work, BYOD and corporate network security

Search

To search, type and hit enter.

Recent Posts

Remote work, BYOD and corporate network security

Gearing up for safe remote work

How CEOs fall victim to hackers. The example of Jeff Bezos

Encrypted e-mail for private use. All you need to know

VPN for private use – a good idea?

VPN for private use – a good idea?

Archives

- April 2020
- March 2020
- February 2020
- January 2020
- December 2019
- July 2019
- June 2019
- May 2019
- April 2019
- March 2019
- January 2019
- December 2018
- November 2018
- July 2018
- June 2018
- May 2018
- April 2018
- February 2018
- May 2017

TestArmy CyberForces

Top IT Services Firms Clutch 2020

Top QA Testing Companies Reliable Company 2020

50 Technology Fast 50 2019 CENTRAL EUROPE Deloitte.

ISTQB Platinum Partner International Software Testing Qualifications Board

Services

- Security Testing
- Vulnerability Assessment
- Red Teaming
- Penetration Testing
- Secure Software Development
- Cybersecurity Program
- Social Engineering
- C-suite Level Management Cybersecurity Services

Industries

- Fintech
- E-commerce
- Software Houses

Company

- Contact
- Blog

Knowledge

- Ebooks & Raports

Connect with us

✉ info@cyberforces.com

+ 48 693 189 866

TestArmy CyberForces Sp. z.o.o.
ul. Petuniowa 9/5
53-238 Wroclaw
Polska