SAGACENT®
TECHNOLOGIES
Cybersecurity, IT Management & Cloud Solutions

Best IT security practices for working from home

I'm one of those fortunate people whose company supports a hybrid work environment. This means that I generally work from home, but can actually work from anywhere (in the office, at home, and on the go). On a typical day, I'm in my home office—where I have access to my company's network and all the same sensitive data that's available to in-office employees. Working this way, security is both a critical success factor and a shared responsibility, as my company and I collaborate to maintain a highly secure cyber environment that safeguards valuable digital assets.

According to a Forbes Jan 23 2023 article, remote working increases the likelihood of data breaches. This was brought home forcefully to employees of The Heritage Company in Arkansas after a failed recovery from a ransomware attack forced the company to restructure and fire 300 workers in 2020.

Best practices for a hybrid or work-from-home model

Once a rarity, work from home (WFH) is now a common way of working (it even has its own acronym!). But WFH comes with its own cybersecurity and logistical challenges:

- How do employers help their remote WFH employees create a secure and productive work space at home?
- How do they make sure the entire hybrid work environment is hardened against attacks?
- How do they ensure WFH security throughout the system: authenticating users, protecting passwords, managing access, and avoiding the potential cross-contamination of laptops, phones, and tablets moving from one place to another?

> The biggest cybersecurity threat to organizations comes from within. A joint study by Stanford University Professor Jeff Hancock and security firm Tessian has found that a whopping 88 percent of data breach incidents are caused by employee mistakes. Similar research by IBM Security puts the number at 95 percent.

In order to stay productive and successful while working from home, it's important to have the right tools and equipment. Coming from an employee who is "working in the trenches," here are some key components that I believe make this new paradigm work:

Password managers let you maintain secure passwords for all your online accounts. If you do a search, you can see a Cybernews list of the best ones in 2023. With a service like RoboForm, which is the one I use, you set things up once, and then never need to remember or enter your passwords again. Security best practices dictate that no two accounts should ever use the same password. No two workers should ever use the same password either.

Device passwords usually come with "administrator" or another generic default password. An important first step is to change these when you install a new router, PC, tablet, etc.

Software versions need to be updated frequently to strengthen security and fix known bugs. Regularly updating VPNs, all devices, as well as all software and applications with the latest software patches and security configurations will plug holes that cybercriminals can potentially use to gain access to your systems.

VPNs or virtual private networks encrypt internet traffic and secure network connections when using a public network. It's important to use the VPN your employer provides when logging in to work systems from home, and never access company data over public Wi-Fi.

Multi-factor authentication (MFA) validates the identity of an individual before giving them access to sensitive data. Companies can make MFA mandatory for their employees if they're accessing critical accounts when working from outside the office.

Plug-in drives can be loaded with malware without your knowledge. It will run on the destination system as soon as they're inserted. Avoid using them if at all possible.

Antivirus/anti-malware programs should be used to keep intruders off your system. Antivirus programs would protect against online threats such as worms, viruses, Trojans, and key loggers; while anti-malware will detect and remove new and sophisticated malware strains and strengthen overall security. However, antivirus and anti-malware software has been replaced by a new generation of endpoint detection and response (EDR) software. EDR is built to detect and deter today's more sophisticated attacks and companies should seriously consider adopting it.

External backups are a critical part of every work-from-home setup. You can do them on inexpensive and easy-to-use external hard drives that physically attach to your system. Or use a cloud backup service that backs up to a remote server. You can program either to do complete or incremental backups every day, or on some predefined frequency. And both should be readily available for restoration in the event of a system failure, an outage, a hack such as ransomware attack, or a natural disaster.

Work-from-home best practices for employers

If you are an employer supporting work from home and hybrid work, here are some things you need to do:

Make security an integral part of your company culture

- Equip remote workers with the tools they need to work productively and securely offsite
- Educate your employees about secure work practices and requirements
- Include the employee's home in your risk perimeter
- Use multifactor authentication (MFA) to verify user identities
- Use a virtual private network (VPN) to provide secure access from anywhere
- Ensure data generated by remote employees is continually backed up

Work-from-home best practices for employees

As an employee working in a hybrid or work-from-home environment, you need to:

- Adhere to all of your company's security protocols
- Use separate computers for work vs. personal activities, using company issued systems whenever possible
- Make sure you have strong remote user/device security
- Password protect all systems and mobile devices, including your router
- Keep current with all system and software upgrades
- Create strong passwords and change them frequently
- Set up your home office for maximum privacy and focus
- Think about security in everything you do

Bad habits to avoid:

- Don’t access or share sensitive data on any platform not approved by your IT team
- Never share passwords
- Always change default passwords on new equipment (e.g., do not use a term like “admin” that hackers can easily guess)
- Don’t store passwords in the open (no lists or sticky notes around your home office)
- Don’t use public Wi-Fi
- Never leave your laptop logged in and unattended in a public place
- Never open an email or file from an untrusted source
- Never use non-company-issued USB sticks on company hardware (and if you use a company-issued USB stick, only use it on your company equipment)
- Run anti-malware and antivirus scans frequently unless these are managed by your IT team
- Don’t forget to do regular backups and store them in a safe place

Managing a hybrid or WFH work environment

According to the latest 2023 cyber crime statistics by AAG, a UK based provider of cloud and cybersecurity services, [the contents of] nearly 1-billion emails were exposed in a single year, affecting 1 in 5 internet users.

As increasing numbers of employees work remotely, employers are helping WFH employees with the office, productivity, and security tools they need to recreate the onsite office experience at home. With a computer or mobile device, a stable internet connection, messaging and collaboration apps, and the right IT support, employees can work safely and productively from a home office or on the go.

Final thoughts about my work from home or hybrid work life

Working remotely has worked out well for both my company and me. At my home office, I find that I can focus with fewer distractions and also be more productive in a secure environment that my IT department has helped me set up. Cybersecurity protection is not a fixed function but requires constant maintenance to address potential vulnerabilities, and I appreciate the strong IT/employee partnership that keeps me up to date and cyber-aware. I view cybersecurity as a shared company/employee responsibility: any breach or hack threatens us both!

Get a graphic reminder

Here is an infographic to download that will remind you of best WFH practices.

Contact Us

2010 El Camino Real #766, Santa Clara, CA 95050-4051
Phone: 408-248-9800 | Fax: 408-248-9700
Service: support@sagacent.com | Sales: sales@sagacent.com | Inquires: info@sagacent.com

SAGACENT® TECHNOLOGIES
Cybersecurity, IT Management & Cloud Solutions

Visit sagacent.com to learn more.

About Sagacent
Founded and Headquartered in San Jose, CA, in 2000, Sagacent Technologies, Inc. is a leading technology solution provider to small and mid-sized businesses offering our customers a full range of solutions.