HP WOLF SECURITY

KEEPING YOU AND YOUR COMPANY DIGITALLY SAFE AT HOME

SECURE YOUR DIGITAL WORK LIFE

TECHNICAL WHITEPAPER

UNPRECEDENTED NUMBERS OF PROFESSIONALS ARE WORKING REMOTELY

INCREASED NETWORK ATTACKS TARGETING HOME WI-FI® NETWORKS AND VPNS MEANS THE NEED FOR HEALTHY DIGITAL SECURITY PRACTICES ARE ESSENTIAL TO ENSURE EMPLOYEE AND ORGANIZATIONAL SAFETY.

TABLE OF CONTENTS

Increased network attacks targeting home Wi-Fi® networks and VPNs, phishing using coronavirus-themed domains that misleads to malicious sites, visual privacy breaches, and productivity impacts are a few threats during these times of vulnerability. While the current situation necessitates rigor around personal hygiene, the need for healthy digital security practices remains equally high to ensure employee and organizational safety alike. This is because the world is simultaneously witnessing unprecedented numbers of professionals working remotely, in most cases from within the confines of their home. As an IT decision-maker, IT security expert or IT admin, incorporate best practices for working remotely using HP capabilities.

IS YOUR COMPANY READY FOR HOME SECURITY GAPS TO BE EXPLOITED MORE BY HACKERS AND CYBER CRIMINALS?

For many people around the world, a new and unexpected phase in their working career begins now – working from home. Under normal circumstances, the ability to work from home comes after the creation of a clear, documented policy that addresses potential issues and concerns and provides guidelines to keep individuals and companies digitally secure. However, with the Coronavirus pandemic we are not living under ordinary circumstances and enhanced guidelines of working from home may not have been fully established yet.

To illustrate, here are some situations that your employees may be facing:

- The security measures implemented in the company network, such as the corporate firewall and anti-phishing security controls, are not present when working from home.
- The router the employee connects through at home is probably not secured and may contain vulnerabilities, since no one monitors it for scanning or backdoor vulnerabilities on a regular basis.
- If your company does not issue a corporate laptop, the employee may use their personal computer. Their computer won't contain security solutions used by your company, may not be actively monitored, and might already contain malware and exploits.
- Working from home might cause a mix of saved passwords between the employee's personal accounts and their company accounts.

However, some professional workers are experienced with working from home, such as when working outside of office hours or on travel. As a result, professional workers do use security tools and IT services provided by their company.

However, three core areas are set to change significantly in the current climate:

1. More workloads will execute outside of IT infrastructural control. In the current environment, devices work predominantly over the internet, where such extensive protection is unavailable. The endpoint is largely out on its own and is only as safe as the layers of protection built into it. IT also doesn't possess the ability to run updates and patches on devices as successfully as they could within the intranet. This means vulnerabilities could potentially remain unpatched for much longer.

2. Remote work security tools and services can become strained. Work-from-home security tools are designed to handle limited traffic and workloads. However, with most of the workforce now remote, the demands from such services are stretched beyond the function for which they were designed. This peak demand can crash critical security services or result in service unavailability for users, reducing company security postures.
3. Employee productivity challenges are expected to grow. During business as usual, remote IT support was used to resolve technical issues. Typically, such activities took time and IT staffing was limited. Now, as more employees work from home, remote IT support needs are increasing, thereby increasing IT costs. Support tools may not be as effective (i.e., when home network connectivity is impacted due to a large remote user base), which causes added delays in bringing the user back to full productivity.

Now your company can easily navigate the constantly evolving threat landscape inherent within the remote working terrain using a set of best practices that you will learn about here.

YOUR COMPANY, SKILLFUL NAVIGATORS IN THE CURRENT SECURITY LANDSCAPE

After the COVID-19 outbreak: Fast-forward to your IT infrastructure operating with instant protection from the moment each of your company's HP machines power on.

With a set of best practices, your company found—and used—the best ways of working to successfully navigate the home-working threats that COVID-19 produced. You stayed current with the ways that effective businesses operated, including measuring the ways of working against those used by the market leaders.

The policies you deployed distributed updates to your machines. Once deployed, built-in features were able to run. Those services provided you with an advanced layer of protection for your endpoints, particularly outside the borders of your corporate networks.

You were able to gain an extra layer of protection in the instances where unprotected users selected weak credentials or shared their credentials inadvertently with bad actors.

This can be your company.

In fact, this will be your company after you've rolled out the best practices that follow. However, before we get into those best practices, consider this fact:

Microsoft Word is the most common malicious file type, with

67% OF MALWARE found within Word files.

(Source: HP Sure Click and HP Sure Click Enterprise Telemetry 2019)

Since the remote workers in your company are more than likely using MS Word to get work done, you'll be relieved to know the best practices that follow can help you. Your company can get ahead of problematic malware and secure the most commonly used programs necessary for ensuring productivity in your company's remote work environment.

Here's another fact to consider:

73% OF MALWARE DETECTED

are Trojans that can carry malicious payloads.

(Source: HP Sure Click and HP Sure Click Enterprise Telemetry 2019)

The best practices you will learn can help your company gain traction against persistent Trojans, avoiding the destructive payloads that they deliver.

The best practices are brought to you by the HP Security Team, a team of committed professionals dedicated to assessing safety risks and security threats that may potentially affect your company and staff.

With that said, HP presents the Working Remote Best Practices, the step-wise guide for helping keep your company and staff digitally safe.

WORKING REMOTE BEST PRACTICES FOR STAYING DIGITALLY SAFE AT HOME

Here are simple, yet essential policies you should roll out immediately to your remote staff:

1. **Practice good digital hygiene.**

   Poor digital hygiene can invite malware that could gain a backdoor into your corporate environment. Since some malware are advanced and persistent, they can go unnoticed for weeks, even months. While your PC may look normal and act normal, it may become a carrier of dangerous malware that could threaten your entire company.

   As part of good hygiene, close off any company applications accessed on your device at the end of each day. Good computer hygiene dictates closing off any company assets accessed on your laptop during your typical day. This practice remains in effect whether the employee is in the office or working from their kitchen table. Even if your workforce has scattered to the wind, make sure they continue to clear their cache regularly.

   On a related note, it's not uncommon for many employees to take advantage of convenient features in their favorite web browser to store their login credentials for sites they visit. While they may do this with their home computers, it is not something you want them to do with their corporate asset.

   If you can, deploy a password storage solution across the workforce.

2. **Minimize use of work computers for personal use.**

   Prolonged use of consumer domains, such as gaming sites, can increase the risk of exposure to malicious attackers. If working from home is new to your employees, ensure they understand that the corporate laptop is for work purposes only.

Of course, you don't need to worry about the employee getting weather or news updates via the computer. What you don't want to find out is that their 14-year-old used it to browse and play games on competitive gaming sites. While the employee's child may have no malicious intent, that use of the computer opens the potential for an attacker to encourage a click on a link or open a document that could silently install a malicious application. If successful, the attacker would have successfully opened a backdoor into a broader corporate environment.

An endpoint security product, such as HP Sure Sense, can mitigate this risk, as it has the built-in ability to analyze and prevent malicious files from reaching a computer's hard drive without any connection to the corporate environment.

3. **Isolate browser tabs into virtual machines.**

Phishing is increasingly a highly targeted activity that follows a bait-and-trap pattern. The bait usually targets something that a user wants to do, such as logging into a banking website or clicking to read a news article related to Coronavirus. The trap is usually to steal end user's credentials/personal information or inject malware into the user's device.

Recently we have noticed an uptick in new phishing campaigns that target employees eager for the latest information on the COVID-19 outbreak. In fact, here's a statistic to highlight the current environment:

COVID19-RELATED DOMAINS ARE 50% MORE LIKELY to be malicious than other domains registered at the same period, and also higher than recent seasonal themes, such as Valentine's Day.

(Source: CheckPoint, https://blog.checkpoint.com/2020/03/19/covid-19-impact-as-retailers-close-their-doors-hackers-open-for-business/)

Phishing emails promise information on new testing facilities, infection maps, or information on new closings in the employee's area. The attacks go something like this:

The employee receives an email from what they think is a trusted source, such as a local news organization or even a trusted friend. The email aims to look legitimate in style and design, often using a trusted logo in the header. The email body will be short (by design), and the attacker assumes that the employee will initially review the email on their phone

Seeing the subject line related to the outbreak, the employee eagerly reads the email and, without hesitation, clicks on a link offering the information noted in the subject line. Unfortunately, instead of getting up-to-date outbreak information, malicious applications may be installed silently on the computer, or the attacker may gain a foothold into the machine to use later.

To protect against malicious downloads, HP recommends use of Sure Click. HP Sure Click can isolate each individual tab into its own virtual container. This protects the Host OS and data on the device from any malware that might enter through a browser tab. As soon as the browser tab is closed, any associated malware is also closed, preventing it from wreaking any damage.

When entering your personal data (such as credentials) into any website, caution should be taken to verify that it is the correct domain and not a fake replica of the original site. There are several tell-tale signs that identify a phishing site, such as use of a generic domain name with the original domain embedded as a keyword within the URL, lack of proper website security, and obvious spelling, grammar and design errors.

LEVERAGE HP SECURITY TECHNOLOGIES THAT ACCOMPANY HP MACHINES.

HP Sure Click is available pre-installed on HP machines. In case you have reimaged your machines, you can also download HP Sure Click using HP Softpaq. Download, install, and activate HP Sure Click on all your users' machines to get the benefit of malware protection when your users are under Phishing attack.

HP Sure Click should be considered a protection augmentation, in addition to Secure Email Gateways that are well positioned to tackle phishing as part of the email server-side security.

Also, since users don't easily switch their preferred browsers, ITDMs would need to follow up with their employees to communicate the security value and benefit of adopting HP Sure Click in order to achieve a superior security posture.

4. Emphasize the need to control what others can see.

Increased use of built-in cameras during long hours of remote work may leave cameras staying active inadvertently. Take precaution by remembering to check the camera periodically and turn on the Privacy Camera Shutter built into HP devices.

5. Ace productivity.

Technical issues impacting company devices could render remote workers unproductive. While issues could be a result of many factors, such as user error, or corrupt or compromised OS or applications, restoring a PC back to the corporate image while having the user data restored from the cloud can go a long way to improving user productivity. Users should keep data backed up on company-provided cloud data storage drives (such as OneDrive).

6. VPN to the very end.

In the age of the Cloud, we routinely access essential company data via Cloud apps. Our task management, product development, and other productivity tools are cloud-based. It is so common today that little thought is given when working in the office. However, when we leave the safe confines of our corporate network, it's easy for employees to forget that it's a dangerous world out there. Ensure every employee knows how to use their Virtual Private Network (VPN) when working from home.

In some cases, the need for a VPN will be evident, since the apps/data itself will be inaccessible without the VPN connection in certain situations. In other cases, employees could be sending sensitive company information into the wild without the VPN active. The answer is simple—when in doubt, use a VPN. Similarly, you need to ensure your network software is also up to date in terms of patches. For VPN as well as business-critical apps, you should enable multi-factor authentication.

With more users needing to connect to work from their homes, the home Wi-Fi® is becoming an attractive target for cybercriminals. It is, therefore, advisable to use the company VPN software when working.

Of course, as the company's VPN servers are unlikely to be designed for heavy workload, employees should connect to them judiciously, such as when accessing sensitive data or key business systems. For uses involving non-sensitive information, or when using specific modern apps with built-in encryption, a VPN may not be needed.

7. **Nix the public Wi-Fi®**

Avoiding usage of a public Wi-Fi® is advised, as it is likely to be a renewed focus for man-in-the-middle attacks.

Corporate machines should be used to the extent possible, as they have the best security capabilities your company can provide. If personal devices must be used, ensure they have anti-malware and VPN software current and running, and try to connect them on a different Wi-Fi® sub-network in the home to minimize chances of lateral moves of malware between those devices.

Without the ability to use corporate VPNs every time, the endpoint is left to its own defenses, which is why ITDMs should decide to invest in the best endpoint security built into the device.

HP PCs come with a set of anti-malware capabilities. HP Sure Start is a fundamental protection against malware that targets firmware, such as BIOS. This service is always on and provides a self-healing BIOS capability in the event the BIOS gets compromised.

HP Sure Click provides advanced scalable isolation where primary threat vectors (such as Word documents) are isolated inside virtualized containers to protect the Host OS and data. HP Sure Sense is a deep learning, AI-based, advanced anti-malware solution that can protect users against new and unknown malware. Together, they form a robust set of protections for users wanting to work safely from their homes.

Even with remote IT tools, it could be time-consuming and cumbersome to get damaged systems (either corrupt OS or compromised OS) back to normal.

With **HP Sure Recover** (and more so with the eMMC based OS Recovery), ITDMs can easily ensure a remote PC can be restored in minutes and return an employee to full productivity.

HP Sure Recover comes built-in to HP machines. If you have reimaged your machine, you can bring back **HP Sure Recover** by downloading it via HP Softpaq. **HP Sure Recover** with eMMC option is a different device SKU and available as a separate purchase.

8. Keep a checklist handy.

Finally, it's essential to provide employees with a simple-to-follow checklist for what they should and should not do when working from home:

DO:

- Only connect to trusted Wi-Fi® connections and networks.
- Only install approved applications on your corporate laptop.
- Maintain communication between your coworkers and manager.
- Inform IT immediately if suspicious activity on a computer is observed.
- Ensure that the only VPN you are connected to is that of your workplace.
- Make sure there is an endpoint security tool installed on your computer and that it is updated and configured correctly.
- Make sure your End Point Protection service can be synced without cloud connectivity, if possible.

DON'T:

- Share your corporate laptops with anyone, even family members.
- Don't connect to a public Wi-Fi®.
- Don't save any company confidential information to your personal accounts.
- Don't leave your computer unlocked at any time, even at home.
- Don't save any company passwords to your personal web browser.

CONCLUSION

As the Coronavirus Pandemic has led us to the current scenario where workers worldwide are turning to working from home, security becomes a very important aspect of this large-scale change. With these Working Remote Best Practices, users and ITDMs can now leverage security technologies built into an HP machine, as well as follow good digital hygiene practices to ensure employees and their company stays safe. Use the Working Remote Best Practices to reinforce your remote workers and company on into the future.

Learn more at: http://www.hp.com/wolfsecurityforbusiness

Sign up for updates: hp.com/go/getupdated

HP WOLF SECURITY

4AA7-7191ENW, June 2021