hp + Windows 10

THE CYBER-SECURITY FIELD MANUAL

Ten steps every business should take to protect against cyberattacks.

Be more secure from power on to power off.

The Cybersecurity landscape is constantly changing and expanding. Small and medium-sized businesses are increasingly having to confront cyberattacks that threaten their information—and their customers' private data. This guide is designed to help those small and medium-sized businesses with limited IT resources to strengthen their cybersecurity today, with little to no cost.

TABLE OF CONTENTS

The Threat Landscape

Cybersecurity Trends in Small and Medium-Sized Businesses

These are five of the top trends in the state of cybersecurity for small and medium-sized businesses, according to the Ponemon Institute[1]:

1

More businesses are being attacked.

In the past 12 months, cyberattacks on small and medium-sized businesses have risen 11%, from 55 percent to 61 percent. The most prevalent attacks against smaller businesses are phishing/social engineering (48%) and web-based (43%). At the same time, cyberattacks are growing more targeted, severe and sophisticated.

2

Attacks are growing more costly.

The average cost due to disruption to normal operations increased 26%, from $955,429 to $1,207,965. The average cost due to damage or theft of IT assets and infrastructure increased from $879,582 to $1,027,053.

3

Human error is a top cause.

Of small and medium-sized businesses who had a data breach, 54% say negligent employees were the root cause — an increase of 48% from last year. However, similar to last year, 1 out of 3 companies in this research could not determine the root cause.

4

Strong passwords and multi-factor authentication remain underutilized.

Passwords continue to be an integral part of cybersecurity. However, 59% of respondents say they do not have visibility into employees' password practices, such as the use of unique or strong passwords and sharing passwords with others — unchanged from last year.

> 59% say they do not have visibility into employees' password practices

5

Malware is growing more sophisticated.

More businesses are victims of exploits and malware that evaded their existing protections, such as intrusion detection systems (66%, up from 57%) and anti-virus solutions (81%, up from 76%).

[1] —Report: 2017 State of Cybersecurity in Small & Medium-Sized Businesses. Ponemon Institute LLC, 2017

The five most common attacks against small and medium-sized businesses.

1 Phishing/social engineering

Social engineering attacks use human interaction to obtain information about an organization or its computer systems. For example, the attacker may pose as a new employee, a repair person, or a researcher. By asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.[2]

Phishing is a form of social engineering. In a phishing attack, the attacker poses as a trustworthy organization, and uses email or malicious websites to solicit personal information.[2]

2 Web-based attacks

In web-based attacks, the attacker gains access to a legitimate website, and posts malware. The legitimate site acts as a parasitic host, infecting unsuspecting visitors. One of the most insidious types of web-based attacks is a "drive-by-download", where the malicious content is automatically downloaded onto a user's computer simply by browsing to the site. No user interaction is required.[3]

3 Malware

Malware is a broad term that refers to any software that is intentionally designed to cause damage to a device or network.[4] This includes viruses, spyware, ransomware, and all the other "-ware"s. Beyond web-based attacks, it can enter a victim's computer via a USB drive or compromised network connection.[5]

4 Compromised/stolen devices

A device that is compromised or stolen can contain both information of value and locally-stored credentials that allow further access into an organization's information and networks. Weak passwords and data encryption can further exacerbate this type of attack.

5 Denial of service attacks

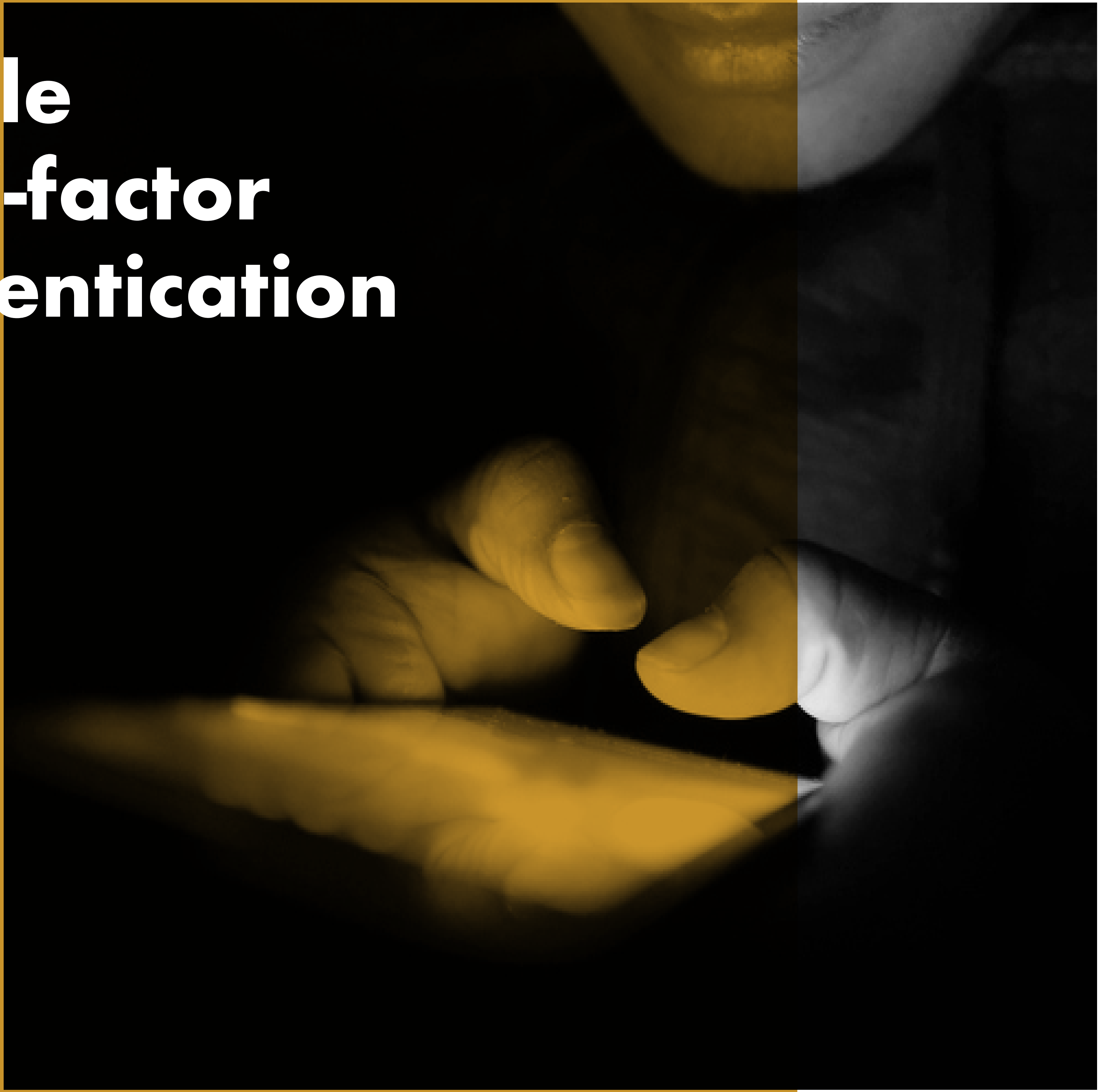
Denial of service attacks are accomplished by flooding the targeted network with traffic until it cannot respond or simply crashes, preventing access from legitimate users. A distributed denial of service attack (DDoS) occurs when multiple machines are operating together to attack one target, increasing the power of the attack. DDoS also increases the difficulty of finding the true source.[6]

2—https://www.us-cert.gov/ncas/tips/ST04-014
3—https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/web-based-attacks-09-en.pdf
4—https://technet.microsoft.com/en-us/library/dd632948.aspx
5—https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf
6—https://www.us-cert.gov/ncas/tips/ST04-015

Ten Ways to Protect Yourself

Section 1:

Enable Multi-factor Authentication



Usernames and passwords are a key target for hackers, and with good reason — your identity is your most valuable asset. Strong and secure passwords go a long way, but passwords alone are not the most secure authentication mechanism. And, in a world of increasingly commercialized hacking, thieves who are not experts can outsource that work to others. Hackers can buy special-built hardware designed for password cracking, rent space from public cloud providers, or create a botnet to do the processing.

- 90% of data stolen by phishing are user credentials[7]
- 80-90% of passwords can be hacked in under 24 hours[8]

Multi-factor authentication (MFA) requires you to use two or more independent credentials to prove your identity, substantially increasing your level of security. Credentials can be something the user **knows** (passwords or PINs), something the user **has** (Bluetooth® phones or smartcards), or something the user **is** (facial or fingerprint recognition). If one factor is compromised or broken, the attacker still must face a second and different type of barrier.

HP MFA and Intel® Authenticate both allow for multiple authentication factors to be required at every login attempt.

[7] —Verizon, 2016 Data Breach Investigations Report, 2016
[8] —Source: Brian Contos, CISO at Verodin, Inc. Quoted with permission. https://www.csoonline.com/article/3236716/authentication/how-hackers-crack-passwords and-why-you-cant-stop-them.html

Set up Multi-factor Authentication with HP.

Modern HP Pro or Elite devices support setting up MFA through the HP Client Security Manager.[9]

1. Open Client Security Manager (you'll need administrator access to do this). If you open it within HPs Manageability Integration Kit (MIK), you can push your MFA policies to your entire PC fleet.[10]
2. From the Dashboard, click on Standard User Policies.
3. Choose the two or three factors for which you wish to configure a login policy, and follow the directions as prompted to enroll the credential or credential pair — such as scanning a fingerprint from the PC's fingerprint reader or entering a PIN.

Diversify with Windows Hello.

Many modern Windows 10 devices with a built-in webcam are compatible with Windows Hello, including the entire range of HP notebooks and convertibles. By scanning your face, Windows Hello provides an alternative to a password as one of your MFA credentials.

1. Open Settings> Accounts> Sign-in options
2. Under 'PIN' select 'Add' if you don't have one set up already.
3. Under 'Windows Hello' select 'Set up,' and follow the on-screen instructions to scan your face.

[9] —HP Client Security Manager Gen4 requires Windows and Intel® or AMD 8th generation processors.
[10] —HP Manageability Integration Kit can be downloaded from http://www.hp.com/go/clientmanagement.

Section 2:

Strengthen Your Passwords

Passwords are ubiquitous in our daily lives. We use them for virtually every personal or professional device, service, and account. As they are the first — and far too often the only — line of defense in protecting identity and data, using bad passwords can have devastating results. Despite this, most people are not using strong and unique passwords.

- 59% know a secure password is important, yet only 41% choose a password that is easy to remember
- 91% understand the risk of reusing passwords, but 55% do it anyway
- Millennials typically use stronger passwords than Baby Boomers (65% vs. 45%)[11]

If your device or service doesn't support MFA, the next best option is making that one password work as hard as it can. Most people do not have strong passwords because they simply don't understand how to create them, assuming it would probably be an arbitrary combination of letters, numbers, and symbols. But there are stronger and simpler ways to dramatically increase your level of password protection.

[11] —Source: LastPass, "New Research: Psychology of Passwords, Neglect is Helping Hackers Win", Katie Petrillo, May 1, 2018

Mnemonic over numeric.

Mnemonic passphrases are more secure than simple passwords, and easier to remember than numeric ones. When used in place of simple passwords, mnemonic passphrases are virtually impossible for hackers to crack.

1 Start with a memorable phrase.

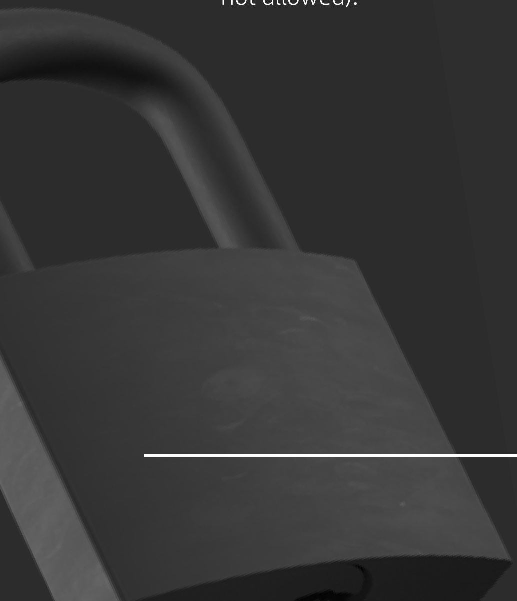
For example, the first six words of Abraham Lincoln's famous Gettysburg Address, "Four score and 7 years ago" is a simple passphrase. The quote meets the majority of password standards: 8-32 characters in length and includes capital and lowercase letters, at least one number, and one special character (the spaces—or underscores if spaces are not allowed).

2 Maximize the weirdness.

Increase the quantity of numbers and special characters used. For example, modify the letters in our previous example to read: "4 $core @nd 7 Ye@rs ago."

3 Customize, don't copy.

By simply attaching a simple suffix to the end of each passphrase, you can reuse your master password easily without the dangers of duplicate uses. For a Facebook account, try adding "FB" to the end of passphrase, or "IG" for Instagram.



Use a password manager.

Password managers are one of the top safety practices recommended by security experts. They work by generating and storing long, complicated passwords for each of your online accounts—freeing you from remembering them. Generally, you'll only need to remember one password: the master password to your "vault". Password manager setup is simple, and the process is usually the same:

1. Download and install the software, and an extension for your browser. You can also download an app for your mobile device.
2. Set up your account with an email address and your master password.
3. Input the details of your various accounts.

Most password managers will require you to manually update your old passwords: log in to your account, go to your account settings, and let your password manager generate a new, more secure password. Replacing your old weak passwords may take time, but the significant increase to your security is worth it.

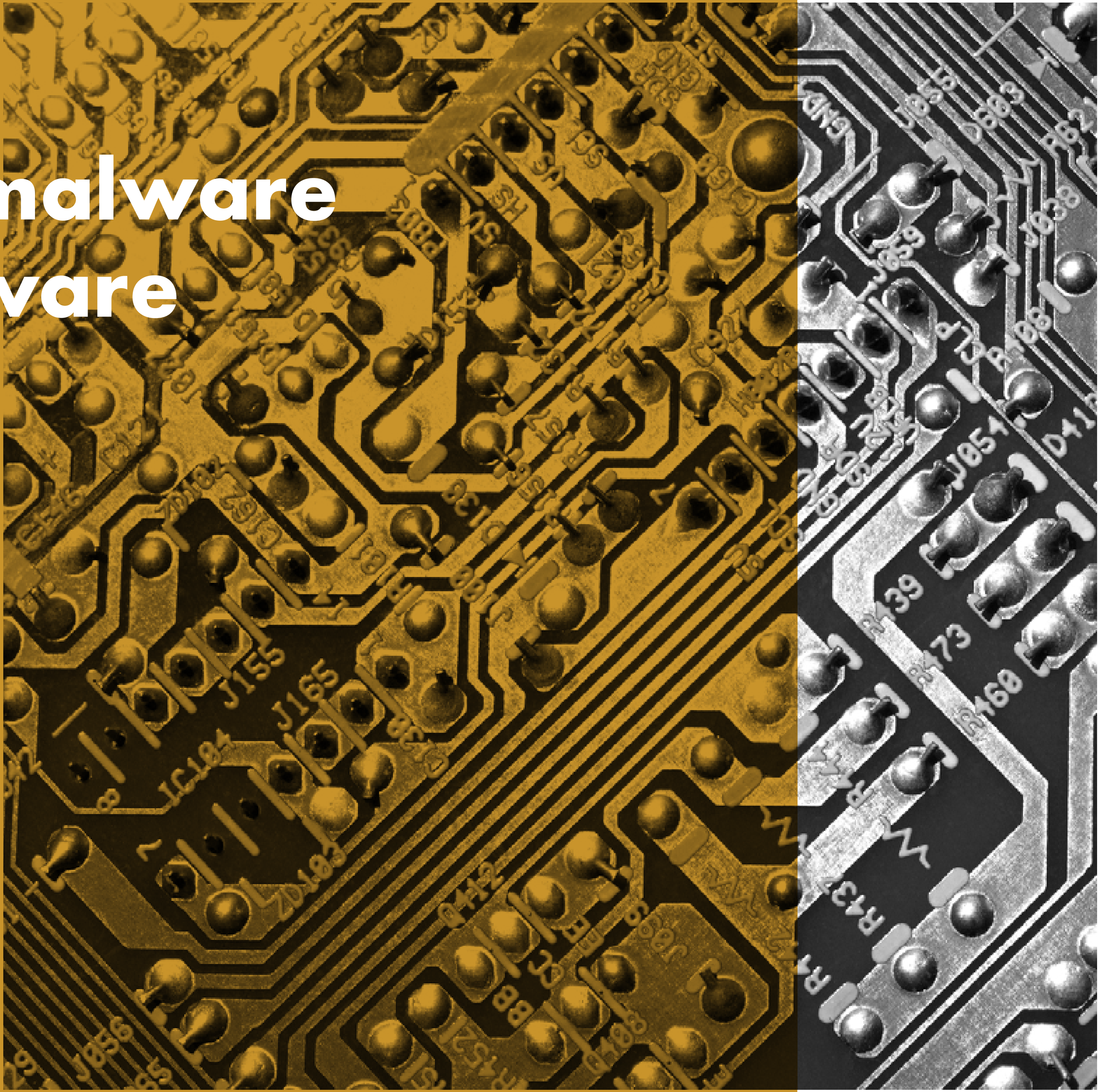
Choosing a password manager.

There are a variety of free password managers available, including Bitwarden, Dashlane, and Enpass. In general, look for a password manager which:

- Integrates easily into whatever browser you use the most
- Allows you to save the password file as an encrypted file, unreadable to users without verifying user identity. Specifically, choose a password manager that uses AES-256 encryption or stronger.
- Allows 2-factor authentication to access password vault.
- Assigns an emergency contact who can also have access to password vault.
- Stores additional login information along with the password (i.e. security questions, phone numbers, account details, etc...)

Section 3:

Use Antimalware Software



Without Antivirus protection, a PC could be infected by malware within minutes of connecting to the internet.

Malware of all shapes can be hosted on seemingly-reputable sites or nested in email attachments, and new malware is being created every day. The bombardment of viruses on your PC is constant, so a tool that protects it must be strong, deeply-rooted, and regularly updated. A good antimalware program is all three.

In a nutshell, antimalware software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses (and other malicious software such as worms, trojans, adware, and more). A typical antimalware program will scan your system on a regular schedule and automatically remove malware it finds, as well as alert you about dangerous downloads and software updates.

Have it, or get it.

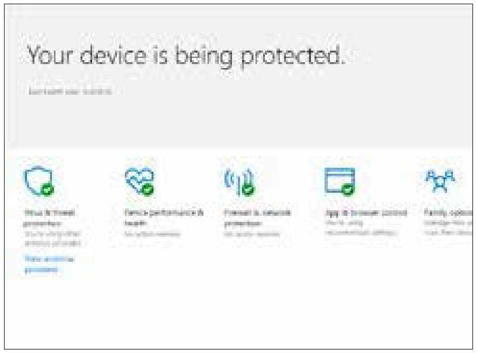
There are many antimalware products available. If you are running Windows 10 on your PC, you already have the Windows Defender Antivirus program installed and running. Alternatively, you can purchase a 3rd-party antimalware program. However, be sure to follow the vendor's instructions to configure automatic updates, so that you always have the most current virus protections applied.

Always be running.

Most importantly, antimalware software must always be running to remain effective. As it is common for malware attackers to first target security programs like antimalware, this step isn't as simple as it may seem. In Windows 10, you can verify whether your antivirus program is currently enabled by checking Windows Defender Security Center.

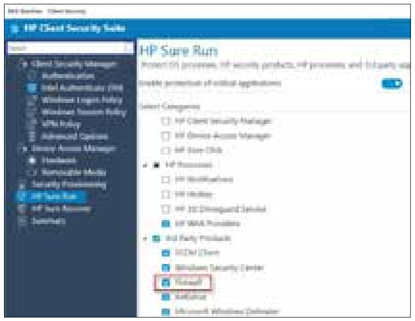
1. From the Start menu, launch Windows Defender Security Center and navigate to Home.

2. Under the setting "Virus & threat protection", if Antivirus is running, you will see a green checkmark. If you're using a third-party Antivirus program, click on "View Antivirus providers" to see additional security details in the Windows Control Panel about your antivirus program status.



And keep it running.

HP Elite products also include HP Sure Run[12], an extra layer of security that ensures that all of your critical processes on your PC, including your antivirus software, remain up and running. Any process that Sure Run is monitoring will be automatically restarted if it's disabled—preventing disabled or crashed antivirus software from leaving you vulnerable.



HP Sure Run must be enabled locally in HP Client Security Manager Gen4.

[12] —HP Sure Run is available on HP Elite products equipped with 8th generation Intel® or AMD® processors.

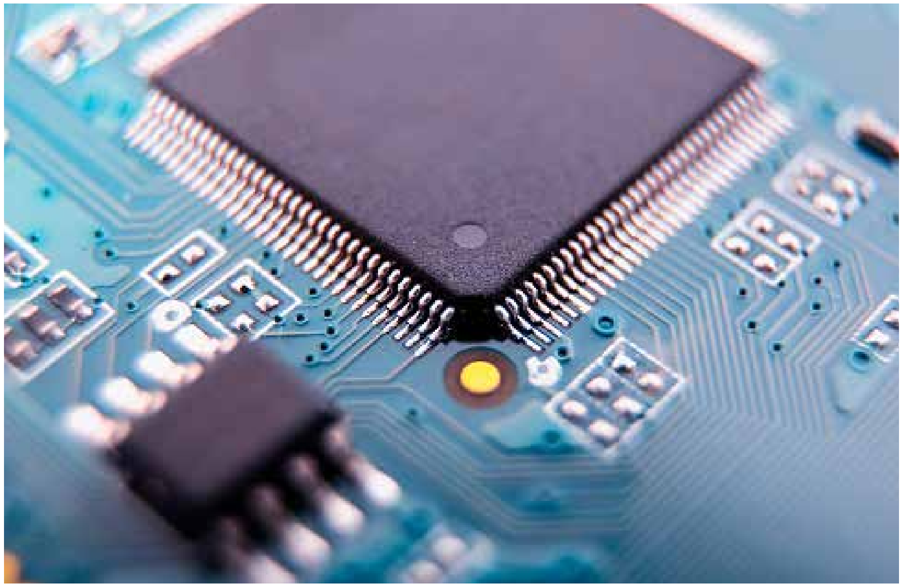
Section 4:

Keep Your Software Up to Date

Antimalware isn't the only kind of software that faces evolving threats—it is important to keep all of your software current. If your software is not up to date, it might be missing important security patches to newly-discovered vulnerabilities. This applies to both the operating system (OS), like Windows®, and all the applications running on the PC, like internet browsers, Office applications, accounting software, antivirus software, etc.

The user also must keep in mind that older or discontinued software may no longer receive security updates. As time goes by, cyber criminals find vulnerabilities in published software and take advantage of these findings. Using the OS as an example, checking for an update on Windows 7 may not present any new software, but that overlooks that Windows 7 is no longer the most current version of Windows. Patching older software isn't the same as updating to the latest version—the older your software, the less secure it is.

> The older your software, the less secure it is



Verify you're updating.

As software vendors find solutions to vulnerabilities, they push those solutions out through software updates. Most applications have an update service built into their software, guaranteeing you are notified if an update or patch is available. Some software vendors even automatically install the updates upon availability. Windows 10, the most current release of Windows (and thus the most secure), has an automated software update mechanism to keep the operating system up to date—and all other Microsoft applications like Microsoft Office as well.

To verify that automatic updates are enabled:

1. Go to settings and choose "Update security."

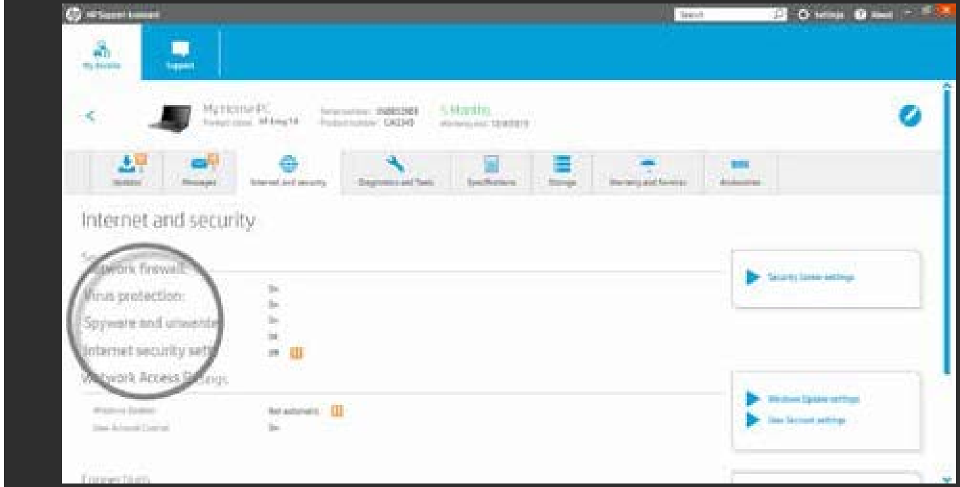
2. Under “Windows Update” choose “advanced options” and ensure that “Automatic” is selected under “Choose how updates are installed.”

3. Ensure that “Automatic” is selected under “Choose how updates are installed.”

Use an update manager.

The breadth of software that comes with your PC can make it tough to ensure *everything* is up to date. For that reason, many PC vendors provide pre-installed tools to automatically collect all the software and firmware updates for the system. On HP systems, this tool is called HP Support Assistant.

For third-party applications, the update feature is often performed by a small update application which is started at boot time. These helper tools make the boot time a few seconds longer, but save you having to browse for updates on the application vendors’ websites. If you have software that doesn’t automatically check for updates, or if you are unsure, check the version number against the developer’s website and update to match if necessary.



Section 5:

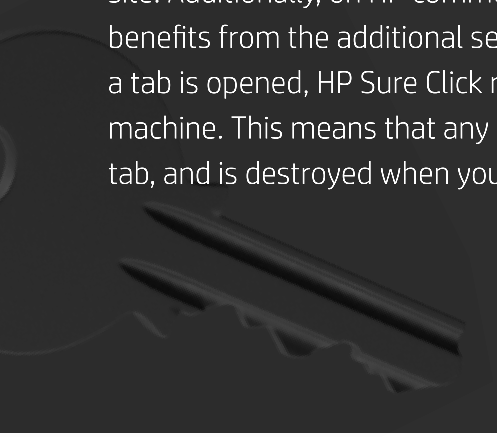
Secure Your Browser

Browsers, such as Internet Explorer or Chrome™, are the #1 way we access the internet—which makes them the #1 target for hackers. These attacks typically come by way of an accidental or intentional click on a link that launches malicious code known as malware.

There are a few simple steps you can take to significantly reduce your chances of a malware attack through the browser.

Use a secure browser.

Internet Explorer, Edge, and Chrome all offer strong security features for Windows. Edge and Internet Explorer 11, for example, use Microsoft SmartScreen to perform a reputation check on each site, and block any they suspect to be a phishing site. Additionally, on HP commercial PCs, Internet Explorer benefits from the additional security of HP Sure Click: whenever a tab is opened, HP Sure Click runs it in an isolated virtual machine. This means that any malicious code is trapped in the tab, and is destroyed when you close your browser[13].



Heed warnings.

Most mainstream and modern browsers have a basic threshold for detecting malicious websites and will display a warning if they believe there to be a reasonable threat. Some also offer URL "autocorrect" features, to prevent navigating to a commonly-misspelled domain (where malicious software and sites are often hosted).

In Edge, go to Advanced Settings> Privacy, and then enable the settings "Use a web service to help resolve navigation errors"

Keep it current.

Enable automatic browser updates through Settings. As previously mentioned, doing so will ensure that all security updates are applied to your browser, making it much safer and increasing the chance that malware attacks will fail.

In Edge, updates are applied whenever Windows updates. However, to check whether you need an update to Edge, go to

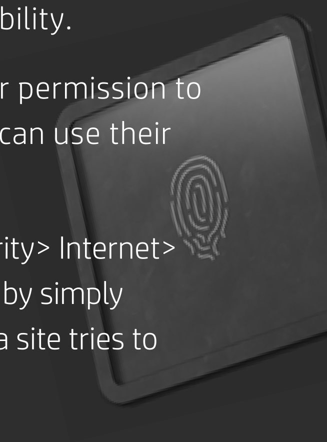
- Start
- Settings
- Updates and Security
- Windows Update
- Check for updates

Restrict content and plug-ins.

Many of these browser add-ons (like Flash or JavaScript) are necessary for rich sites and web programs, but their increased access to your system also makes them a vulnerability.

Disabling them by default requires a site to ask for permission to use them, and ensures only sites you opt to trust can use their features.

In IE, go to Tools (gear icon)> Internet Options> Security> Internet> Custom level...> Scripting. You can disable JavaScript by simply selecting "Disable," or you can request IE ask before a site tries to use it by selecting "Prompt."



[13] —HP Sure Click is available on most HP PCs and supports Microsoft® Internet Explorer and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read only mode, when Microsoft Office or Adobe Acrobat are installed.

Section 6:

Router Security & Private Network

The router is the first line of security from intrusion into any network. Anyone that connects to the internet does so through a router. This hardware device, either wired or wireless (Wi-Fi®), allows communication between the internet and your local network (i.e., your PC and possibly other connected devices). As such, enabling the highest level of security on the router is the best way to keep your PCs, printers, and data safe from malicious attack.

> Routers were cited as the most frequently exploited type of device in IoT attacks.[14]

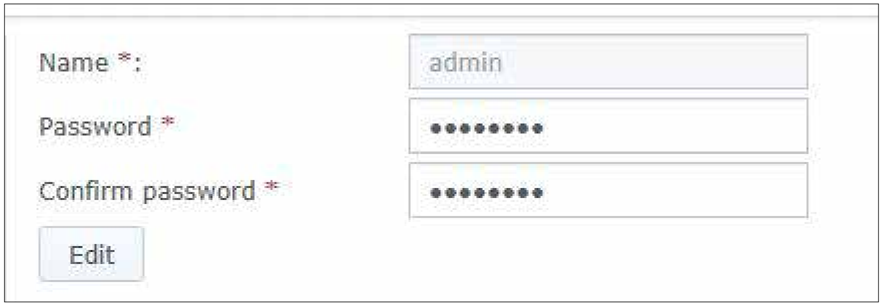
Because routers transmit ALL the data that flows in and out of your home or business, including email and credit card information, routers have long been a favorite target for hackers. In Symantec's 2018 Internet Security Threat Report, routers were cited as the most frequently exploited type of device in IoT attacks. Hackers can use malware or design flaws to hide their identity, steal bandwidth, turn your devices into botnet zombies—or worse. They can also then take advantage of any unsecured devices.

14—Source: Symantec Corporation, 2018 Internet Security Threat Report, 2018

Secure your network.

Unfortunately, many vendors continue to offer both unsecured and secured router configurations. If a router is unsecured (that is, allowing connections to it without requiring an administrator password), anyone could connect to the router and thereby jump onto your local network. A hacker could change your passwords, spy on you, or even access the files on a network-attached hard drive.

Always secure your routers with non-default administrator passwords using the tips from Section 2: Strengthen your Passwords. Below is a screenshot of how most routers allow you to set passwords to secure them on the network.



Name *: admin

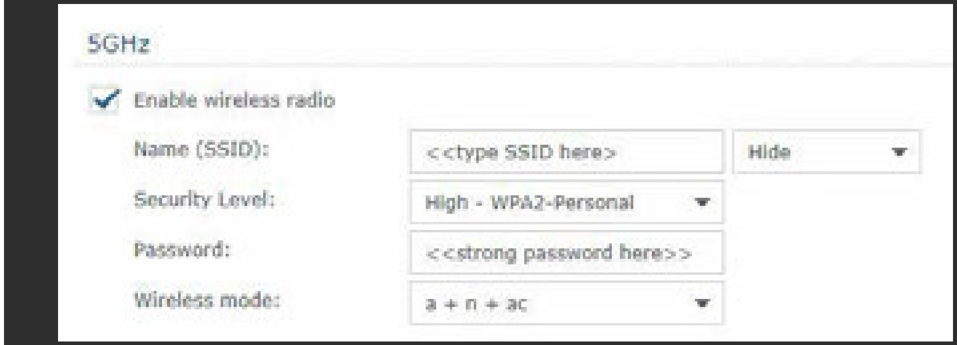
Password * ●●●●●●●●

Confirm password * ●●●●●●●●

Configure encryption.

With wireless routers, passwords are only half the battle—choosing the proper level of encryption is just as important. Most wireless routers support four wireless encryption standards: WEP (weakest), WPA (strong), WPA2 (stronger), and WPA3 (strongest). Go with the highest encryption standard supported by your router.

Below is a screenshot of how to set the appropriate level of encryption on your router. To do so, you need to login as the router administrator and navigate to the encryption settings (varies by router vendor).



5GHz

☑ Enable wireless radio

Name (SSID): <<type SSID here> Hide

Security Level: High - WPA2-Personal

Password: <<strong password here>>

Wireless mode: a + n + ac

Keep the firmware up to date.

Many router manufacturers roll out software updates throughout the year to address security problems. Just as we discussed with PC software, a router with the latest updates is much less likely to be infected by malware. Most router vendors apply firmware updates automatically without requiring customers to perform this operation. Newer router models may also offer a mobile app, which you can download to a phone just like any other app and use to check for updates. However, if automatic firmware updates are not offered by your router vendor, you should navigate to the router manufacturer's website, go to Support, and identify the correct update based on your router's specific model name and ID (typically found on the router itself).

Use Virtual Private Networks.

Going beyond securing the hardware inside your business, a Virtual Private Network (VPN) is a server that you connect with to reroute your external internet activities. VPNs can protect and secure your identity and information. The goal of a VPN is to provide a mainstream way to browse the web privately (but not always anonymously). All the traffic that passes through your VPN connection is secure and cannot, in theory, be intercepted by anyone else—meaning they're great for use on both local networks and public ones. More on VPNs and their benefits in Section 7.

Section 7:

Protect Yourself on Public Wi-Fi®

Today, public Wi-Fi® is near ubiquitous. Airports, local bars, shopping malls, even outdoor parks offer free internet access via hotspots. They're incredibly convenient—and dangerous.

Users connected to these hotspots share the same network—meaning there's a real chance someone could take advantage of the unsecured traffic. A hacker can even set up a hotspot and try to lure people on to their (similarly-named) spoof network. This can allow eavesdropping on unencrypted data streams or execution of man-in-the-middle attacks to bypass encryption.

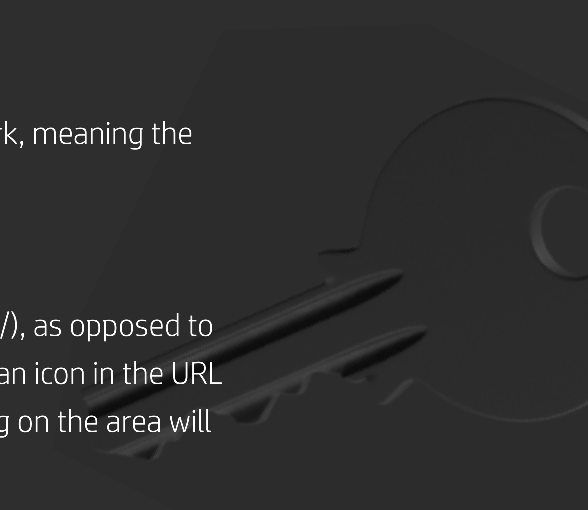
It is important to always presume your communications are unsecured and public when using an open network. However, should there be no other option, there are ways to reduce your exposure.

Limit your activity.

Don't transmit highly sensitive material like company documents, emails, or passwords, and don't use any type of banking/ accounting applications or portals.

Look for a plan B.

If possible, use semi-open networks that are at least password-protected. These are usually a managed network, meaning the provider has an interest in keeping the network secure (i.e. airline lounges)



Stick to encrypted sites.

Ensure you are connected to a web server which supports encrypted traffic through the HTTPS protocol (https://), as opposed to the unsecured, plain text HTTP protocol. Check the head of the site's URL—a modern browser will usually have an icon in the URL bar indicating when HTTPS is present and the certificate is valid (often a padlock icon or the color green). Clicking on the area will bring up a dialogue further detailing the level of encryption.

Route everything through a VPN.

As we mentioned in the previous section, a VPN can help protect your data when you can't trust your network connection—and a public Wi-Fi® network is a perfect example. A VPN tunnel encrypts your data from end to end, ensuring a would-be interceptor is unable to interpret your activity. Not all VPNs are created equal, so you'll need to choose the right one for your price point and device type. Free VPNs often have limited available bandwidth and simple encryption protocols, meaning you'll experience slower browsing speeds and could still be exposed. That being said, in a pinch, a reputable free VPN is likely better than no VPN at all.

Section 8:

Stop Visual Hackers

Visual hacking occurs when sensitive information is displayed on screen in public places and business competitors, identity thieves, or unscrupulous individuals see, capture, and exploit it. Even the casual curious onlooker is a potential threat. Everything from passwords and account numbers to financial data and proprietary company information is at risk—and no amount of security software can prevent these data voyeurs from sneaking a peek.

As the modern workplace continues to move outside traditional offices to remote and public spaces, the possibility of being "visually hacked" is more real than ever. In fact, visual hacking may be the most underrated, low-tech threat businesses face today. It's simple, effective, and often goes unnoticed until it is too late.

According to research published by the Ponemon Institute[1]:

- 91% visual hacking attempts were successful
- 68% of visual hacking attempts went unnoticed by the victim
- 52% of sensitive information was captured directly from device screens

Be aware of your environment.

When working in public spaces, always assume that someone could be looking over your shoulder and choose tasks accordingly.

Limit your exposure.

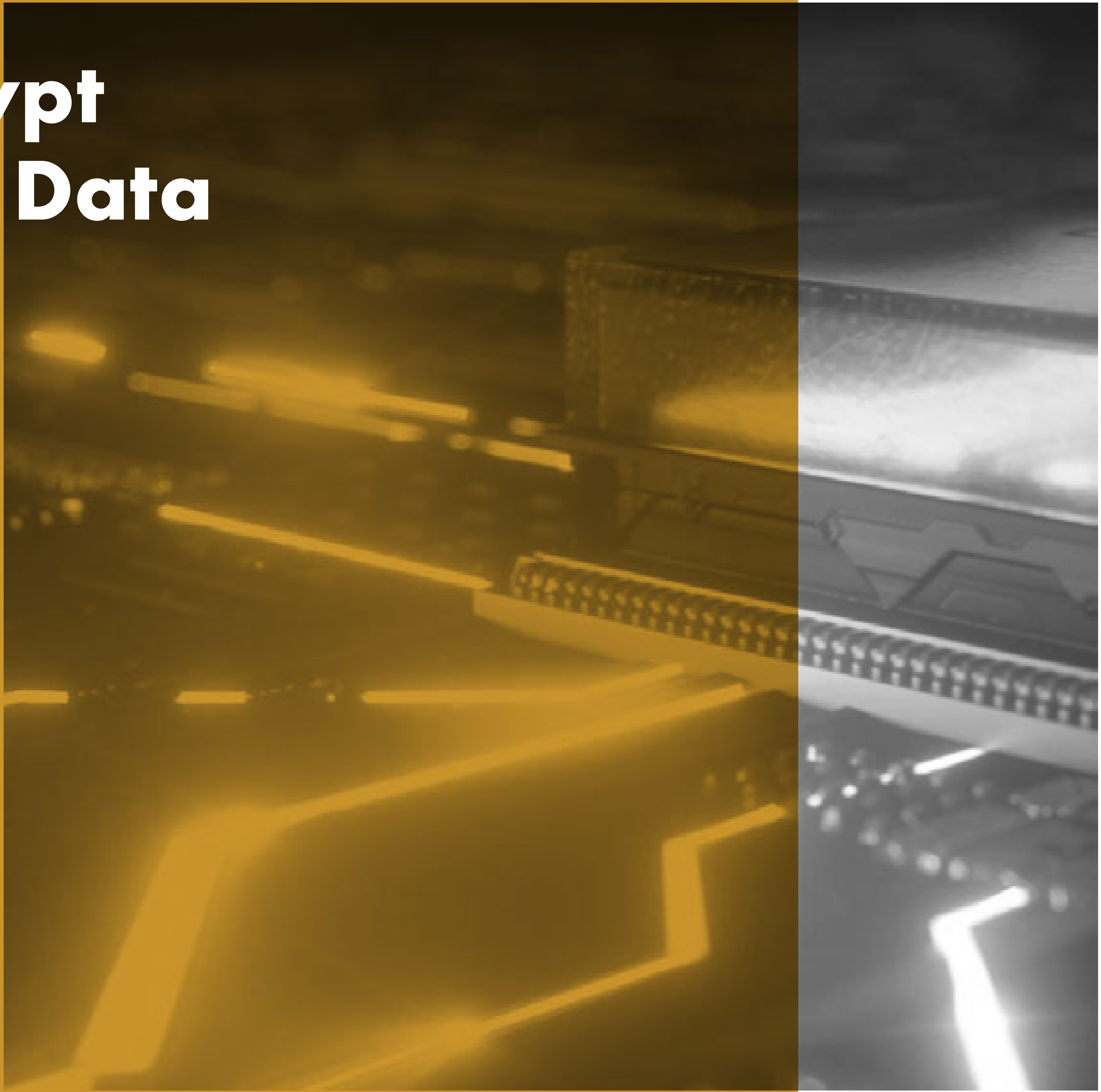
Privacy screens are designed to reduce the screen viewing angles, such that a would-be visual hacker cannot see what is being displayed without being directly behind it. An external filter is a simple way to add this security. It attaches over your display and can be removed when you need to share your screen with a larger audience.

Alternatively, an integrated privacy screen simplifies this process, while removing the need to apply, store, and replace an external protector. Many HP PCs offer HP Sure View Gen2[15], an integrated privacy screen designed to deter visual hacking, as an option. It works by dynamically modifying the structure of the LCD pixels at a molecular level—allowing it to be enabled or disabled with the press of a button, and improving performance in both bright and dark environments.

15—HP Sure View integrated privacy screen is an optional feature that must be configured at purchase and is designed to function in landscape orientation.

Section 9:

Encrypt Your Data



When a PC is lost or stolen, the hard drive is the first point of attack. Only a few screws hold it in place, and once removed, it can be mined on another PC. If you haven't properly protected your data, reading a drive is like cracking open a book.

Encryption ensures that whatever is mined remains completely unintelligible. Encryption is the process of encoding data to make it unreadable by anyone who does not have the secret decryption key. So a computer with an encrypted hard drive can be stolen but not accessed—a far better outcome than having your corporate or personal information in the wrong hands, forever.

Enable software encryption.

Windows 10 supports password encryption of your hard disk using your login credentials as the key. This ensures a hacker would need your username and password to access your data.

Ensure you have a strong password for your user account:

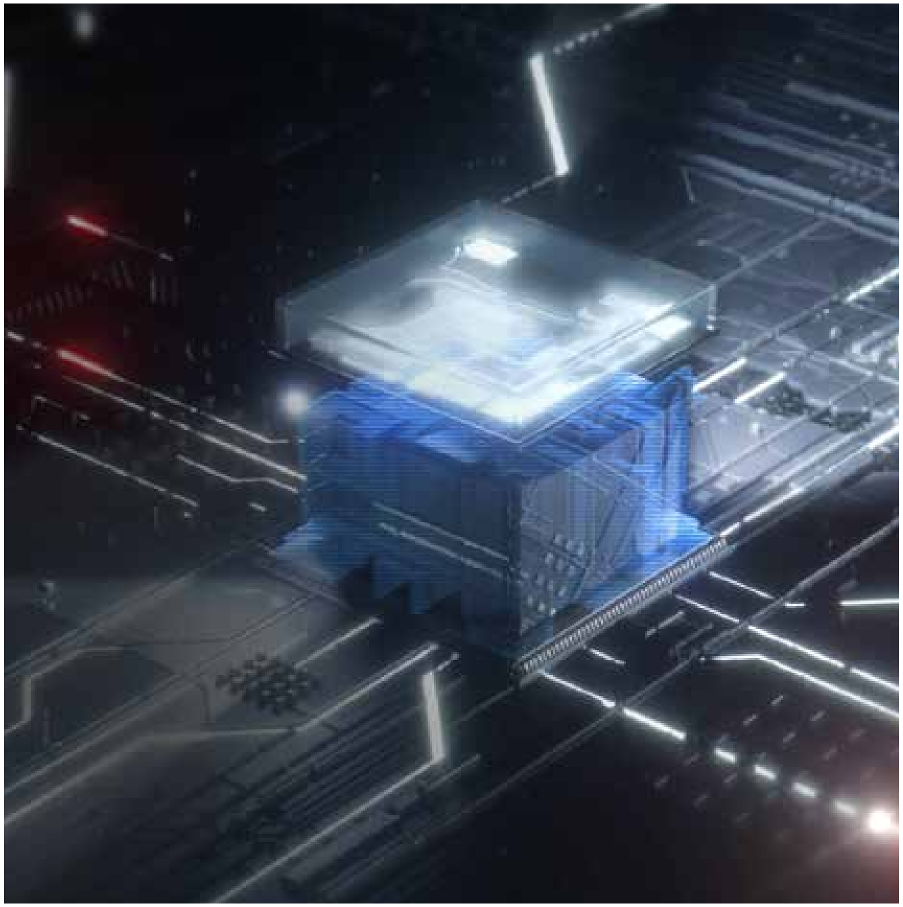
1.
   - Settings> Accounts> Sign In Options> Password

2. If available, turn on Trusted Platform Manager (TPM), which activates a security chip within your PC to encrypt your new passwords and data on the drive:
   - Settings> Update & Security> Windows Security> Device Security> Processor

3. Turn on Encryption, ensuring your data cannot be viewed or copied without your credentials:
   - Settings> Update and Security> Drive Encryption

Take advantage of hardware encryption.

BitLocker is a feature of Windows 10 that provides software encryption that is unlocked with a hardware key. Devices that have a TPM chip, like HP notebooks, can encrypt without extra hardware. The TPM prevents access to encrypted data if it detects the system has been tampered with while turned off. Devices without TPM can use BitLocker as well, but require a removable device, such as a USB drive, to serve as a key.



Section 10:

Secure Your PC Below the OS

The BIOS (Basic Input Output Software) is software that boots a computer and helps load the operating system. By infecting this core software, spies can plant malware that remains live and undetected by antivirus. It remains even if the hard drive is erased or or operating system re-installed.

If a hacker gains access to your BIOS, they essentially own every aspect of your PC.

This gives the attacker a way to exfiltrate data or brick the system by modifying the firmware, which would require replacement of the entire system board to repair. For HP Elite and Pro PCs, HP Sure Start can automatically self-heal the BIOS from malware, rootkits, or corruption, adding an extra layer of protection and creating a trusted foundation for your PCs security[16].

Leave no update behind.

As mentioned earlier in section 4, software updates ensure that newfound vulnerabilities are patched—and the BIOS is no exception. As most BIOS implementations share the same source code across a workforce or user base, any discovered vulnerability is likely present in many implementations across the PC vendor landscape. OEM tools like HP Support Assistant will check for updates automatically, or you can check your manufacturer’s site for BIOS updates.

Dig into the BIOS.

The BIOS factory settings can be seen as a balance between security and usability. However, to protect the system against the many possible methods of transferring malicious code, you may want to remove some of that functionality.

How to access the BIOS settings can vary slightly from manufacturer to manufacturer, but it usually is done by pressing a function key during initial boot up (F10 or FN-10 on HP notebooks).

[16] —HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel® or AMD processors.

Set a BIOS password.

To protect the BIOS settings from being changed by unauthorized users, it is recommended to set a BIOS password:

- For Example: Security> Administrator Tools> Create BIOS Administrator Password

It is important to remember the BIOS password, as it is designed to not be circumvented or recovered.

Set a Power-On password.

For even greater security, a Power-On Password can be created. Anytime the PC is turned on, before the system runs anything, the Power-On Password is prompted. Like the BIOS password, this too cannot be easily recovered or reset, and forgetting it renders the machine unusable.

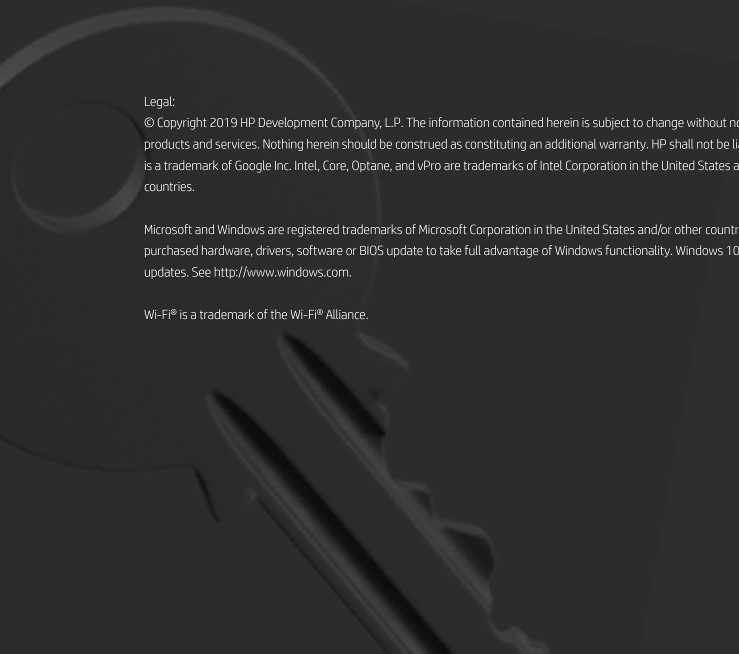
Limit unused features.

In BIOS, there are a few settings to consider for maximum security. While they may remove some functionality or reduce accessibility, the below-OS security they enable cannot be equally replicated with software:

1. Remove external and optical devices from the boot order (Ex: Advanced> Boot Options). Especially USB Storage Boot, Network (PXE) boot, and optical drive boot, as these allow for malware to be loaded from external sources. If booting from these devices is needed, the feature can be turned on case by case.
2. Disable Legacy Support (Ex: Advanced> Secure Boot Configuration) and enable Secure Boot.
3. Activate the feature “Save/Restore GPT of System Hard Drive” (Ex: Security> Hard Drive Utilities).
4. Enable DriveLock and set a password.

Conclusion

Today, more digital threats are targeted at small and medium-sized businesses than ever before. The good news is, much of the hardware and software you own contains underutilized security features to help combat them. There are also an unprecedented number of products and services available with state-of-the-art security innovations to protect against tomorrow's unknowns. From hardware-based security on contemporary devices to self-updating software, a smart investment on connected, secured devices now will pay dividends deep into the future. HP designs security solutions that capitalize on the strengths of Windows 10, supporting the built-in security features with discrete hardware augmentations and always-up-to-date software support. The threats you face are evolving daily—and the right security strategy substantially increases your odds against them.



THANK YOU.

To learn more, visit: www.hp.com/go/windows10now

hp + Windows 10

Be more secure from power on to power off.