Whitepaper

HP Business PCs—Security Best Practices for IT Professionals

Introduction

HP is taking steps to combine industry-wide best practices for cybersecurity with HP specific recommendations for our IT professionals. This collaborative effort with HP security professionals provides proactive security measures to secure industry PCs.

Implementing best practices provided by HP, IT professionals can achieve a higher level of protection in their environment from potential malicious or unauthorized access attempts.

This document is subject to continual reviews and updates. Check back for updates to this and other sections.

General Best Practices for the IT Professional

Table 1 General best practices for the IT professional

Action	Additional notes & reference
Secure your PC	• Setup BIOS Administrator Password NOTE: if using BIOS Administrator Password, customers may choose to set the “Clear Password Jumper” setting to “disable/ignore” if their particular security environment requires it. (Applies to select Desktop Business PC’s only). If this option is chosen, be sure to remember or safely store the password(s). Reset all the BIOS settings back to factory defaults to ensure they are using the best settings HP recommends if the security environment requires this • On Intel vPro systems: Set the MEBX password (may require setting the BIOS Administrator Password on select systems) • On AMD® systems with DASH management: The Realtek NIC has a password that should be set / changed from its default • For Windows 8 and later: Ensure that Secure Boot is enabled • Ensure that your default boot path does not include external media prior to booting the internal hard disk Keep up to date with the latest firmware and software. You can use HP Support Assistant, HP Client Management Solutions, or HP Image Assistant (for Business PCs including Workstations). Additional Protections on select models: Enable GPT protection: If Malware tries to corrupt the GUID Partition Table (GPT), this setting will restore it upon next boot. On Desktops: Engage Chassis/Hood Lock where available On Notebooks: Use Kensington Lock where applicable Enable Sure Start BIOS Settings Protection (on systems with HP Sure Start) For more information regarding the security of your environment, visit HP Go IT, a centralized collection of resources for business IT customers.

Action	Additional notes & reference
Update BIOS	Keep up to date with the latest firmware. Can use HP Client Management Solutions and HP Image Assistant (for Business PCs including Workstations). Sign up for an HP Subscription for notifications or updates on the latest technology, new products and solutions, promotions and events, and driver and support alerts. HP Notebook PCs - Updating the BIOS (Basic Input Output System) HP Desktop PCs - Updating the BIOS (Basic Input Output System)
Update HP device drivers	The HP Image Assistant (HPIA) is recommended. To learn more about and download the HPIA, visit HP Image Assistant. Microsoft System Center Configuration Manager (SCCM) To learn more about HP Solution with SCCM visit HP Manageability Integration Kit (MIK) for Microsoft System Center Configuration Manager. For more information on managing and installing driver updates, visit HP Go IT, a centralized collection of resources for business IT customers. Sign up for an HP Subscription for notifications or updates on HP device drivers. Keep up to date with the latest device drivers. You can use HP Support Assistant, HP Client Management Solutions, or HP Image Assistant (for Business PCs including Workstations).
Enable Endpoint Protection Solutions	For more information about protecting your PC environment, visit HP Go IT, a centralized collection of resources for business IT customers. HP Sure Sense[1] is available on select HP Business PCs and Workstations. Refer to the Software and Drivers section under "Support" at HP.com to find an available HP Sure Sense Softpaq for your device. HP PCs - Installing and Updating Antivirus Software to Protect Your HP PC HP Fraud Alert: Protecting Yourself from Scams
Perform backup on regular basis	OS restoration solution for potential recovery is recommended using HP Sure Recover[2]. For more information regarding the security of your environment, visit HP Go IT, a centralized collection of resources for business IT customers.
Sign up for HP driver and support eAlerts	To be notified and receive support product eAlerts, driver updates, and Security Bulletins, sign up for an HP Subscription.
Visit HP Security Bulletins	Archive site and bookmark for future reference for the HP Security Bulletin Archive. To initiate a subscription to receive future HP Security Bulletin alerts via email, visit HP Subscription.
Practice email security	Phishing protection: Do not open email attachments from unknown source or provide personal information. Malicious attachment protection: HP Sure Click[3] can help protect against malicious email attachments in common Office documents. HP Sure Click is available on many HP Business PCs, Workstations, and Retail Point of Sale systems. Refer to the Software and Drivers section under Support at HP.com to find an available HP Sure Click Softpaq for your device. For more information, refer to HP Sure Click Infosheet and HP Sure Click Whitepaper. HP Fraud Alert: Protecting Yourself from Scams
Improve web browser security	HP Sure Click can help protect against malware encountered while browsing the web. This includes drive-by download attacks and watering hole sites. HP Sure Click is available on many HP Business PCs, Workstations, and Retail Point of Sale systems. Refer to the Software and Drivers section under "Support" at HP.com, to find an available HP Sure Click Softpaq for your device. For more information, refer to HP Sure Click Infosheet and HP Sure Click Whitepaper.

Action	Additional notes & reference
Keep your PC up to date	Updating the to the latest HP Drivers and BIOS has many benefits that include: Security, Performance, Compatibility, Functionality for the HP PC. Sign up for an HP Subscription for automatic product or driver updates and security updates. Get connected with updates from HP Keep up to date with the latest firmware, software, and drivers. You can use HP Support Assistant, HP Client Management Solutions, or HP Image Assistant (for Business PCs including Workstations). Updating Drivers and Software with Windows Update
Encrypt your storage drive	Microsoft BitLocker is included with Windows and provides additional protection for the data on your storage drive. Should your PC become lost or stolen, this can help prevent the data from being accessed. BitLocker Basic Deployment

General Security Recommendations for PC and Internet Use

- Protect sensitive information using HP Sure View Integrated Privacy Screen to help prevent side-angle viewing from onlookers (available on select PCs). For existing systems, HP has Privacy Filters available that can be purchased to help protect your screen from prying eyes HP Privacy Filters.
- Protect your PC from malware that lurks on malicious websites or malicious email attachments in common Office documents with HP Sure Click Infosheet and HP Sure Click Whitepaper
- Use "HTTPS Everywhere" plugin that will provide additional security when browsing the internet, for more information visit HTTPS Everywhere
- Use caution when accessing public Wi-Fi networks. They are less secure than a private, personal one, or a WiFi hotspot that is password secured. When using public WiFi networks:
  - Don't download or install anything new (including videos and music)
  - Read any terms or conditions related to using the public WiFi
  - Select trusted well-known public networks
  - Take consideration of what you are sharing, like any personal details on individual websites
  - Use a secured VPN when working on business-related issues that may include confidential information or accessing sensitive web sites, such as those related to banking or healthcare.
- Protect against malware with HP Sure Run[4] and HP Sure Sense
- Protect your PC using a consistently updated antivirus/spyware protection software program
- Never use the same password for multiple accounts, use password variation by generating them at random. Even better, using a password manager can help by using both strong passwords and unique passwords. HP has a solution in HP Client Security Manager, which is included on many HP Business PCs. Refer to the Software and Drivers section under "Support" at HP.com, to find an available HP Client Security Manager Softpaq for your device.
- Do not store a list of accounts and passwords locally on your PC in a file that can be easily identified or write them down and store in an unsecured location.
- Consider two-factor password authentication. This may require an additional item to access files. This could be an app on your smartphone, a USB drive, or a smart card.
- To learn more about multi-factor authentication: HP Client Security Manager multi-factor authentication
- Do not open emails or email attachments from unknown sources.

- Do not provide personal or credit card information to an unknown source request.
- Enable automated updates for software for keeping your software and firmware up to date.
- To be notified and receive support product eAlerts, driver updates, and Security Bulletins, sign up for an HP Subscription.
- Protect your PC using a consistently updated antivirus/spyware protection software program.
- There may be software settings in the operating system or other additional software that can provide added security settings for kids and family use.
- Only download software or drivers from trusted websites. Be careful when downloading free software from sites that prompt for personal information in order to download.
- Be security aware and research common security issues: U.S. Department Of Homeland Security - Tips
- For recommendations on corporate security: The Best Ways to Improve Corporate Cybersecurity

Mitigating Security Best Practices

Mitigating security risks

- How can you mitigate the security risks?
  - Do not open links or attachments, or provide sensitive information, in response to suspicious emails, instant messages, or phone calls
  - Verify that the message and sender are who they claim to be:
    - Was I expecting this message?
    - Do I recognize and trust the sender?
    - Does the context of the message make sense?
    - Hover your mouse cursor over the link (do NOT click) to discover its true destination
- Still not sure? Verify the message by using a trusted phone number (do NOT use the contact details in the original message)

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

[1] HP Sure Sense requires Windows 10. See product specifications for availability.

[2] HP Sure Recover is available on HP Elite PCs with 8th generation Intel® or AMD processors and requires an open, wired network connection. Not available on platforms with multiple internal storage drives or Intel® Optane™. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data.

[3] HP Sure Click is available on select HP platforms and supports Microsoft Internet Explorer, Google Chrome™, 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.

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