HP Remote Worker Cybersecurity Best Practices

With the Coronavirus (COVID-19) pandemic affecting so many people, we are reaching out to let you know your safety and security are in our thoughts.
Many employees are now working remotely. Just like good hygiene helps ward off COVID-19, it is important to not overlook cybersecurity hygiene. Here are important strategies and tips for protecting employees, systems, and company data during this time, reducing the risk of an accidental or malicious security breach.

Managing the big picture

- **Corporate Information Security Governance**
  Review your current cybersecurity governance policies to ensure security guidelines for remote work and remote access to company information systems are adequately outlined for your employees. These guidelines may be in a formal information security policy, if your organization already has many remote workers. They may also be covered in your resiliency or disaster recovery plans, or in bring-your-own-device (BYOD) policies, where employees usually have to opt into a set of corporate mandates and policies if they use their own devices to access company systems and data. If no policy exists or your cybersecurity governance is not adequate, this is the right time to establish a well-considered policy.

- **Formal Organization Security Communiqué**
  Managers should be very familiar with applicable security guidelines, security plans, and policies, and ensure that pertinent information is shared with their respective teams and throughout the organization. It is critical that all levels of the organization are aligned on cybersecurity hygiene, and essential to remind employees they are accountable and responsible for adhering to the company's cybersecurity guidelines and policies. This is a good time to send a companywide security communiqué to remind everyone of your cybersecurity recommendations and requirements.

- **Security Event Preparation**
  Each organization should review its formal incident response plans to ensure readiness to respond to a cybersecurity event. Update the plans as necessary, and where the COVID-19 pandemic has created a requirement to work remotely, include contact information for the remote incident response team. Using remote workers increases the security risk and increases the need to have a formal plan if there is a cybersecurity event such as a data leak or an intrusion.

- **Privacy and Data Protection Laws**
  A variety of privacy and data protection laws continue to apply, even during this COVID-19 pandemic. A number of Privacy and data protection regulators or authorities have provided guidance via their websites for managing personal information during the COVID-19 pandemic. If the GDPR applies to your organization, for example, a number of European Union data protection authorities have issued guidance relating to COVID-19. We recommend reviewing your data protection authority's website or seeking legal advice from your legal advisor.

Checking and communicating the details

To help you get started with sharing remote work cybersecurity guidance, we have provided some information below, we hope you find it timely and valuable to help you in these challenging times.

- Consider which processes and functions are business critical and prioritize these in your risk mitigation endeavors. Revisit your business continuity and disaster recovery plans and ensure that key business processes can be maintained by remote workers. Adapt the policy and processes if necessary. During this endeavor, investigate which corporate functions and roles are now remote that have never been remote before.

- Revisit and enhance your data classification rules and policies and remind employees of the various types of data and company information they must safeguard. Leverage technical security controls wherever possible (e.g. strong encryption, in transit and at rest). Consider whether you wish to allow confidential information such as source code, or strategic documents, to be accessed remotely.

- Ensure that the authorized devices used by your workforce filter applications, websites and services to ensure that potentially hazardous websites or applications cannot cause harm.

- Provide easy ways for your employees to communicate securely on their computers and mobile devices. This can include email encryption and secure mobile messaging apps.

- Ensure that your system backups are operational, have been tested, are viable, verified, valid and are operational and are adequately separated from production systems. Consider the need for efficient data recovery in case of a security event, including a ransomware attack. Ensure employees back up data, preferably in the organization's designated and endorsed cloud environment. If the data is sensitive, ensure when it is backed-up, the data is encrypted.

- Ensure that your security personnel have the tools to carry out incident response activities and other cybersecurity activities (e.g. reverse engineering, forensics) remotely.

- If the office is left unmanned, make sure that no confidential information is left physically unprotected.

- Remind employees of the various types of data and company information they must safeguard. This may include trade secrets, confidential information, intellectual property, information classified as a work product, customer and employee information, and other personally identifiable information.

- Also remind employees that scammers are perpetually on the prowl. They need to be aware of the possibility of phishing attacks, and the many forms of social engineering, and how to protect remote devices and remote access to company information systems. Train employees on how to identify phishing attacks and other forms of social engineering and what to do to protect themselves, their loved ones, and the organization. Scammers are already using phishing emails that prey on public health fears surrounding Coronavirus (COVID-19).

- Encourage employees to change passwords immediately if there is even a hint the password was compromised.

- Do not ever allow the sharing of laptops, computers and other devices. Sharing work devices (such as with family members when working remotely) reduces accountability and increases the risk of unauthorized access to protected company information, even if it is inadvertent.

- For those working from home, recommend keeping the office laptop, office printer and any office network on a separate isolated network away from any other smart home devices such as Alexa, Nest, Ring, or smart TVs. Most Internet providers by default offer a guest network.

- Remind employees to never save or download the organization's information to personal devices. Examples of such devices can include their personal laptop, tablet, phone, thumb drives, and cloud services such as a personal Dropbox or Google Drive account.

- Require security software such as antivirus on employee devices, and ensure this software is up to date and fully patched.

- Remind employees to change settings so that "Remember password" functions are unequivocally turned off when employees are logging into company information systems and applications from their personal devices. Allow no exceptions to this requirement.

- Implement and enforce multi-factor authentication (MFA). If your organization has not yet turned on MFA, this is the right time to do so, in order to reduce your overall security risk.

- Ensure sensitive information is encrypted during transmission, while processing, and at rest. This includes encrypting removeable media.

- Make sure employees use Virtual Private Networks (VPNs), which will encrypt traffic traveling over the Internet. This is especially important when employees connect to a public Wi-Fi network. However, if your organization does not have VPN software, avoid having users download free VPN software. Consider prohibiting employees from accessing company information systems while on any public Wi-Fi.

- Require all employees working remotely to log out when they are not using their devices, including laptop, PC, tablet, phone, and so on. Failing to do this could lead to a security event or a data breach, with the consequential notification requirements.

- Ensure your home office printer has the latest security updates. Subscribe to alerts from your print vendor (such as https://www.hp.com/go/alerts).

- It is strongly recommended to approach protected information with a zero trust model and allow no access to systems unless unequivocally required for an employee to perform their role and responsibilities

- If applicable, consider Mobile Device Management (MDM) and Mobile Application Management (MAM). These solutions may help both manage and secure mobile devices and mobile applications. It is important to note MDM and MAM tools allow organizations to remotely implement a number of security measures, including data encryption, malware scans, and wiping data on lost and stolen devices.

- Remember this time is going to put more strain on your IT and Cybersecurity functions. It is important to fully support these teams, which includes keeping them healthy and well-staffed. Continuously monitor and manage to help keep the organization running.

- Ensure a safe and secure work environment. Employers have obligations under federal and state safety laws to provide a safe and secure environment for employees, and this extends to remote work. The remote workspace is treated as an extension to the regular workforce for safety requirements.

- It is important to reinforce company culture, collaborate and gather teams together to provide support and reassurance. Do not lose sight of the human element in cybersecurity hygiene.

- Ensure employees' WIFI is protected with a strong passphrase (WPA2) and ensure employees have set a strong password on their router.

- Employee routers, computing devices (PC, phone) and print devices must have the latest updates installed. If possible, have employees configure all their devices to enable only the needed functionality. For instance, if a smartphone app requests a respective employee's location and this does not provide added benefit, deny the location request.

.

- Ensure employees set an administrative password on their home printer's web interface and ensure that it is not internet facing. Consult the manual.

- Whether an employee transmits, processes, sends or stores data, ensure it is adequately protected, and leverage encryption. This applies when using any computing devices (e.g. email encryption) and conducting mobile communication (e.g. secure messaging app). Direct personnel to your organization's IT helpdesk for guidance.

- Remind employees to be vigilant and to be aware of scams leveraging the COVID-19 pandemic and to be very cautious of any email regarding COVID-19 which requires action on the employee's part (For examples: downloading an attachment or clicking on a link).

If you would like to speak with your HP Security Advisor regarding these recommendations, cybersecurity hygiene, or any other cybersecurity matter, please notify your account team so we may set up a conversation.

Sign up for updates
hp.com/go/getupdated

Share with colleagues