Always Designing for People™

Work from Home Data Security Best Practices

As COVID-19, commonly referred to as the coronavirus, continues to spread many employees may need to work from home. While the health and safety of our ADP associates and our clients is our number one priority, we must also be mindful of the data security risks that are present when working remotely. Below are some simple best practices you can use whenever you work remotely:

Do Not Use Unsecured Personal or Public Wi-Fi

If your Wi-Fi network is not properly protected, you are exposing your devices to possible malware or ransomware attacks that could allow hackers to monitor network traffic or access files on connected devices. To prevent this, make sure your Wi-Fi network has a strong password and change it regularly. Whenever possible, try not to connect to public networks especially if the device being connected contains sensitive data.

Always log on to your employer approved laptop by using a Virtual Private Network (VPN) to best protect your information and data against malicious attacks.

Avoid Working on a Personal Device

You should only conduct business on a company approved device. You should never allow anyone else to use your work devices, including family and friends. While they may not have malicious intentions, they may unknowingly transfer or publicize confidential data.

Never Transfer Data Using an Unapproved Platform

It's no secret that emailing documents from your work email to your personal email may be the easiest and quickest way to transfer data, but it is also the riskiest way. Personal email accounts lack the protection to securely store data, and data can be stolen or viewed while in transit as well.

Similarly, you should not use a personal cloud account to transfer data. It is not secure and should not be done. There is a chance that you may sync work documents to your personal cloud account without knowing it. Be sure to check your personal cloud account often and permanently delete any work documents accidentally stored there.

Do Not Use an Unsecured Conference Call Line

Only use your company approved conference call platforms. Using online platforms risk exposing your employer to malicious attacks or spreading confidential information to the wrong parties.

It's also important to remember some physical security best practices as well! Remember to:

Pay Attention to Sight Lines

If you are working in a public setting like a café or library, be aware of your surrounding area and who can see your screen. You may think that no one is paying attention to what you are working on, but you can never know who is around you and what their intention may be. If you are looking at sensitive information such as social security numbers, make sure no one can look at your computer screen while you work.

Lock Your Doors

This is good advice even if you are not working from home, but make sure if you need to leave your devices at home to lock the doors to your house before leaving and if possible, also lock the door to the room where you plan on leaving your device.

Do Not Take Physical Copies of Confidential Materials

You should never take home confidential documents or print out confidential documents at home unless absolutely necessary. If you must, make sure to return all materials to your office for proper disposal – never just throw confidential documents in your normal trash.

If you are concerned about the speed of your at-home internet connection, **make sure to stop non-essential web surfing like using social media or video streaming**, and **only use video conferencing when absolutely necessary**.

Clients are encouraged to visit our website at www.adp.com/trust to learn more about how ADP protects data, and how clients can help protect themselves. Protecting our clients and their data from malicious activity is a top priority for ADP.

Sign up to have new alert notifications delivered to you by email – visit the alerts section of www.adp.com/Trust for more information.