Best Practices for Securely Working Remotely

With the recent global pandemic, many organizations have been required by government mandate to have their workforce relocate to their homes. To continue conducting business many employees now find themselves working from home, many for the first time. While it may be an afterthought, it is critical to continue to be vigilant about information security when working outside of the office. This paper will give some best practices, advice and tips for employees, organizations and system administrators to safeguard their organizations information assets.

Employees Working from Home

As many of us find ourselves working from home, maybe for the first time, I recommend the following as you settle into a new routine.

Separate your Work and Personal Activities – It can be very tempting to pay bills, do some quick online shopping, or check social media for a quick break from work activities. While it may seem harmless, these activities can potentially expose your computer to malware or other infections compromising security on the computer you are using for work. These compromises will potentially expose the company assets you are accessing with your computer while working. If you have a computer provided to you from your company, ensure you are only using it for conducting work activities and do not use personal devices for work purposes. Do not use personal email or cloud-based file storage for work purposes as this can introduce additional threat vectors to you or your company's assets. Force yourself to use personal devices to engage in non-work-related tasks. If you are in a position where you have to use your own device to work and connect to organizational systems, consider creating a separate user account that is only used for work activity.

Be Aware of your Surroundings - You may not be the only one in your household that is being forced to stay home, which can lead to having a hard time finding a quiet place to work. While it may seem a bit paranoid to safeguard your work computer and screen from family members or close friends, make sure you are adhering to company policies with regards to who is seeing the data you are working on. If your organization does not have formally defined policies, take a clear screen approach and make sure that you are locking your computer when you are not using it to keep it secure from others in your home.

Keep Software and Antivirus up to Date – This is always a best practice, but bears repeating, keep all software and antivirus updated with the latest patches and definitions. Patches are critical for securing discovered vulnerabilities in applications and having the latest virus definitions will ensure that you are giving yourself the best chance to stay protected. If your organization deploys operating system patches from a server on premise at your office, reach out to them to see how you can continue receiving critical security patches while out of the office. Many patches are released as a result of known vulnerabilities, and not having them applied makes you extremely vulnerable to attack.

Be Cautious about Phishing Emails – Times of crisis like the current pandemic are leveraged as an opportunity for bad actors to gain unauthorized access to systems. Taking advantage of individuals uncertainty and anxiety is a common tactic used by those seeking to gain access to sensitive company data and personal information. These attacks could come in the form of emails from individuals you

work with who have already been compromised and may be crafted to seem like legitimate requests due to the sudden shift of everyone working remotely. These could also appear to be from federal or state agencies urging response in order to receive benefits or critical safety updates. If you receive any email that seems suspicious, especially with instructions to click on links or open attachments, make sure you are reporting them to your IT or security team for their review prior to clicking on anything.

Make your Home Internet Connection as Secure as Possible – If you utilize wireless internet at your home, please configure it to use the most secure wireless settings available on your hardware. Also ensure you have a strong passphrase configured. If your company has made a VPN connection available to you ensure that you are using it even if it is not required to access the assets you need. Doing this will ensure your traffic is encrypted and cannot be intercepted by those who may be listening in on your internet traffic.

Continue to Follow Company Policies – It is just as important to follow your organizations security policies when working remotely as it is when you are in the office. Ensure you are familiar with your organization's expectations, specifically regarding remote access, using personal devices for work purposes, and backing up and saving work data. It is natural to only be concerned with being able to conduct business remotely, but it is still paramount to do it in a safe manner. If you are unsure if something you are doing is secure or not, reach out to your system administration or helpdesk and ask.

Organizations and system administrators

With an emphasis on getting users up and running remotely it is critical to continue to make security a priority. Here are some recommendations to continue to keep your users productive and data secure.

Communicate your Expectations and Policies to your Users – As alluded to above it is critical that your employees understand what is expected of them when working out of the office. If your employees don't know the policies of your organization regarding information security and remote access they cannot and should not be expected to follow them. This is a great opportunity to reach out to all staff with a refresher on relevant policies, where they can find them, and who they should ask if they have questions. If formal policies are not in place this is a critical time to at least determine some guidelines concerning working remotely and communicate them as soon as possible. Specifically provide guidance on how they should be connecting to company assets, if they are allowed to use personal devices to conduct work, expectations regarding safeguarding devices used for accessing company assets, and clear direction on who to contact with questions or concerns.

Highlight Security as a Priority During this Chaotic Time – Information security is most likely not at the top of employees lists of concerns as they are hastily trying to get up and running from home. It may also not be the top priority of management as organizations struggle to stay open and generate revenue in an uncertain climate. Make sure to communicate to staff the importance of safeguarding company assets and information during this time, as well as clearly identifying methods of contacting appropriate personnel with questions and concerns regarding security when working remotely. Again, make sure staff know the expectations surrounding working remotely and provide them links to where they can review relevant policies and procedures. Emphasize adherence to policies which are not enforced by a technical mechanism but are reliant on end users working within the requirements of documented policy on their own accord.

Provide Training Content – This may be the first time many of your employees have had the opportunity to work from somewhere outside of the office, which can be overwhelming for many. To ease the anxiety that comes along with drastic changes provide online training to your staff. The training should include practical advice for assisting them to be able to work remotely, as well as security focused content relevant to the new reality of working from home. Include relevant threats related to working remotely and those associated with the global pandemic and bad actors who would seek to use the situation to gain access to your assets. Most importantly provide users methods and people for them to contact if they need assistance getting up and running or have concerns related to security. If users do not know where to turn for help, they will most likely not report concerns or issues and use their own means to continue to access what they need to complete their work. This can lead to unreported security incidents and unauthorized methods of accessing company information assets.

Utilize Technical Controls Wherever Possible – Having technical measures in place to enforce company policy is the safest way to ensure that remote users are safely accessing organizational information. Requiring encrypted VPN connections to access company assets is recommended to alleviate the risks associated with who may be able to listen in on network traffic originating from your employee's home connections. Requiring multi-factor authentication will mitigate several risks related to phishing and other potential methods of user credentials being obtained by attackers. Disk encryption on employee computers is highly recommended to protect data that resides on devices that will be more exposed to potential theft or loss as they are removed from company property. Enforcing endpoint policy compliance such as ensuring that remote devices connecting to company networks have approved antivirus and up to date signatures before being allowed to connect reduces the risk of infected endpoints connecting to organizational systems and propagating malware. These are only a few examples of technical safeguards, however wherever they are available it is recommended they be utilized. Many users don't know when they are potentially compromising information security and having safeguards like these in place go a long way to prevent mistakes or ignorance from turning into costly breaches.

Evaluate New or Changed Risks for your Organization – A major shift in your users working remotely can expose your organization to new risks that were not relevant when employees were working in the office. This is particularly critical if your organization did not previously have regular remote workers and you have had to make changes to organizational systems to make them accessible remotely for work to continue. Take the time to evaluate the changes that have been made to enable business to continue and potential risks that are associated with enabling the various types of remote access. If you have a formal change control process continue to utilize it. Think through the different roles in your organization and the systems they are now accessing remotely, is additional encryption required? More stringent user authentication? Do you have the ability to enable multi-factor authentication that had not previously been utilized? Whatever the case may be, include security as a factor when evaluating if a change made for remote access is complete.