MYTECH PARTNERS

Providing the best IT experience in North America

Acknowledgement & Transfer of Risk – Remote Access with Personal Devices

Non-corporate owned and managed devices present a significant and very real risk to a corporate network. This document is to provide an overview of well-known risks associated with personal devices being used to connect to corporate resources and data. Our goal is to ensure that any one of our clients choosing to allow remote access to corporate resources from personal devices are fully informed and aware of the risks so you can factor those variables into your decision. Here are some of the known risks associated with remote access from personal devices.

Limited to No Security

– Personal devices will not have the same level of security applied compared to corporate owned and managed devices. Even if all your applications are hosted or Software as a Service (SaaS) there are concerns of which you should be aware.

- No systematic/managed Operating System or Application updates - these updates are the first step toward fixing the security vulnerabilities that are present on any laptop or desktop, and personal machines are not managed with the same diligence your corporate owned devices are managed.
- Basic or no security tools installed - personal devices do not have the same layers of protection and security tools installed that help protect your corporate owned and managed devices. This means that a Bad Actor could infiltrate the system more easily AND remain completely undetected while exfiltrating personal and/or corporate information.
- Key Logging Software – if your organization does not leverage Multi-Factor Authentication, there is an increased risk of a vulnerability/exploit/infection on a personal device that could be used to capture credentials which can be leveraged to log into your corporate network, and/or other hosted and SaaS applications.
- VPN Connection from a Personal Device – if a personal device is used to create a VPN connection to the corporate network this is essentially the same as bringing that personal device to the office. Any and all malware infections/exploits that exist on that personal machine are now INSIDE your corporate firewall and are able to infiltrate other systems in your corporate network.

Violates Regulatory Compliance

– For those industries that are regulated by FINRA, SEC, HIPAA, PCI, DFARS, ITAR, etc., allowing a personal, non-managed, secured device to access and connect to corporate data and resources violates all security regulations that apply to businesses. The risk of compromising access to your data is real and we do not recommend sacrificing convenience of using a personal device over security of individual data in your care.

We understand the that the current extraordinary circumstances require extraordinary actions, and Mytech is working to do our part to keep you, our client safe. This scenario is especially dangerous when bad actors know that the convenience of leveraging personal devices in a crisis will create opportunity for them to exploit (which bad actors already have exploited) this situation.

Mytech Recommendation

– IF a personal device is the only option for remote access, do NOT use a VPN to access the corporate network. We have identified an alternate *and interim* remote access method that mitigates the risk of VPN access from a personal device and can be deployed quickly and cost effectively $10/computer/year.

Acknowledgement and Assumption of Risk

– After being advised of the above risks, I want to proceed and/or continue leveraging VPN as the method of remote access from personal devices. I am asking Mytech to facilitate VPN access on personal devices against security recommendations and best practices.

Signed_____ Title_____

Printed Name_____ Date_____