

8 Tips To Protect Remote Workers




In recent times businesses have quickly made adjustments to allow employees greater flexibility in working remotely. This presents challenges, not the least of which is data-security. Cybercriminals are aware of this new weakness and are aggressively making moves to exploit it. Action must be taken to secure these network endpoints and ensure that businesses can progress through this challenging new era.

TOPICS

- Security Policies
- Patching
- Visibility
- Authentication
- Incident Response
- Antivirus
- Backup
- Education

SECURITY POLICIES

1



As personal and work-worlds collide, there may be an impulse to use every-day filesharing, messaging and project management tools. Local software installations further complicate matters. And security concerns recently brought to light regarding videoconferencing platforms has generated controversy and reminded us that the IT administrators must make it clear which tools have been vetted and authorized for official use. Technology outside of the SysAdmin's realm management cannot be accepted into the environment.

HOT TIP

SysAdmins must work with management to create a remote-work policy that employees can understand and sign-off on as part of their off-site work strategy. This policy should outline important environmental factors that include storage devices, Internet access, filesharing, passwords, support and more.



PATCHING

2

How are you tracking which devices have been updated?

All operating systems, applications and communications technology must be updated with the current security patches. This includes software like web-browsers, collaboration tools like Microsoft Teams and whatever is being used for videoconferencing.

HOT TIP

Implementing a patch management strategy that includes regular inventory of devices, steps for updating and ongoing vulnerability assessment can often be made easier by using a patch-management software platform. Network administrators can then require a system health check be conducted and passed before access is granted to the company network.

VISIBILITY

3

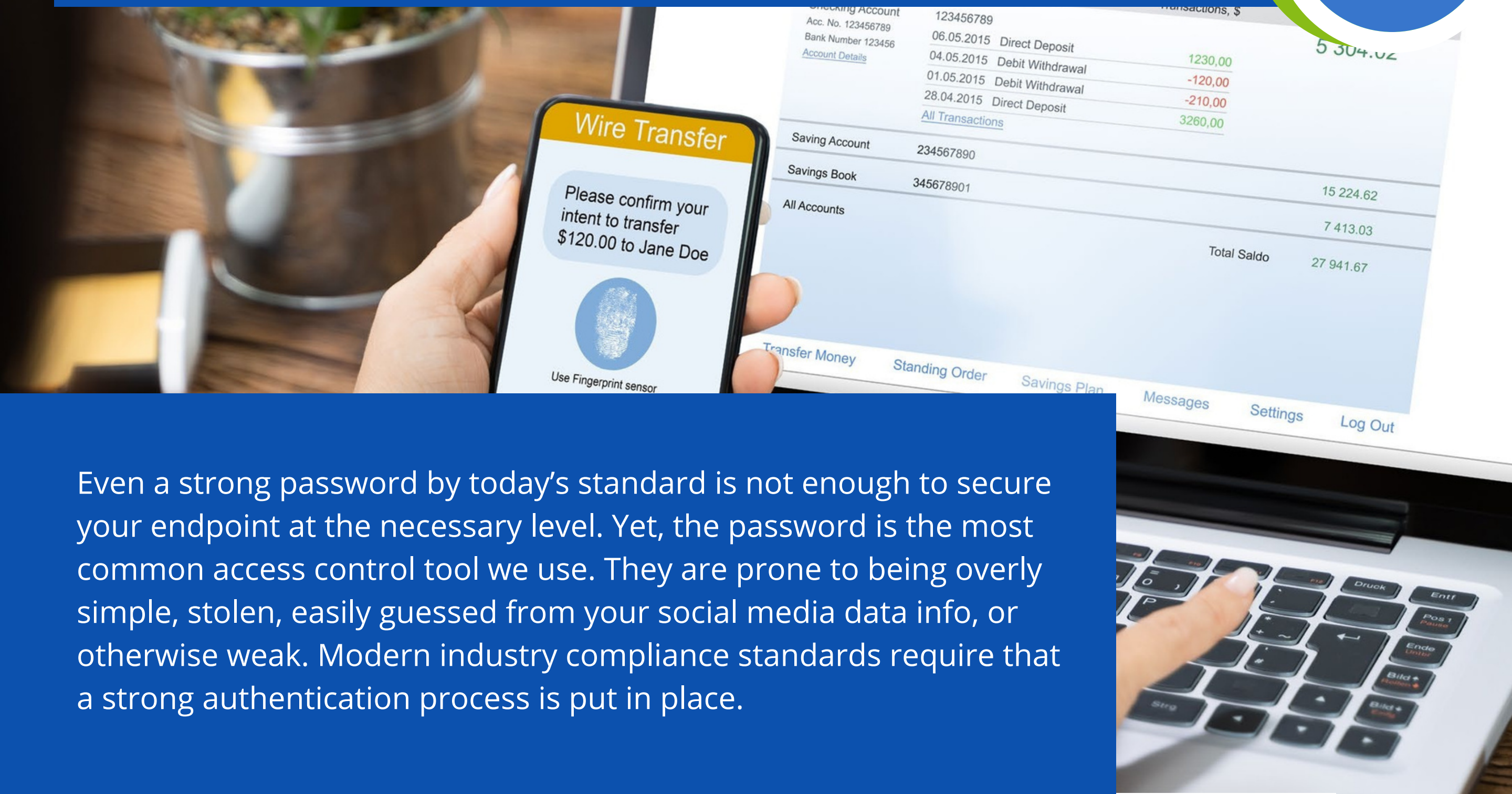
Making your endpoints less visible to hackers is critical to threat prevention. Employees working from home must be able to conveniently access resources (data storage, software, etc) in the same manner as if they were physically seated in the office. Duplicating resources in these remote environments is inherently costly and less secure. When remote employees access public WiFi services, they also become vulnerable having data intercepted by criminals.

HOT TIP

One security measure can greatly reduce the risk of data breach and still allow for mobility — a Virtual Private Network (VPN) with encryption. A Virtual Private Network (VPN) creates a secure point-to-point tunnel between the remote employee and the company network. Data is encrypted making it unusable even if it were intercepted.

AUTHENTICATION

4



Even a strong password by today's standard is not enough to secure your endpoint at the necessary level. Yet, the password is the most common access control tool we use. They are prone to being overly simple, stolen, easily guessed from your social media data info, or otherwise weak. Modern industry compliance standards require that a strong authentication process is put in place.

HOT TIP

Remote workers must provide multiple pieces of information to prove who they are. Asking a personalized question prior to the standard log-in can exponentially improve security. But true implementation of multi-factor authentication means combining passwords with personal data, personal devices (cell phones, memory cards), and/or uniquely personal features such as voice or fingerprint recognition.

As many as **45%** of remote employees don't know how to respond during a ransomware attack. As such, the response from the technical team to a remote employee's malware infection or data-breach must be swift. Employees must resist the urge to battle ransomware on their own, and get the IT department involved immediately. All employees must know when it is wise to isolate their system (disconnect from the network, storage devices, WiFi) as a best practice response.

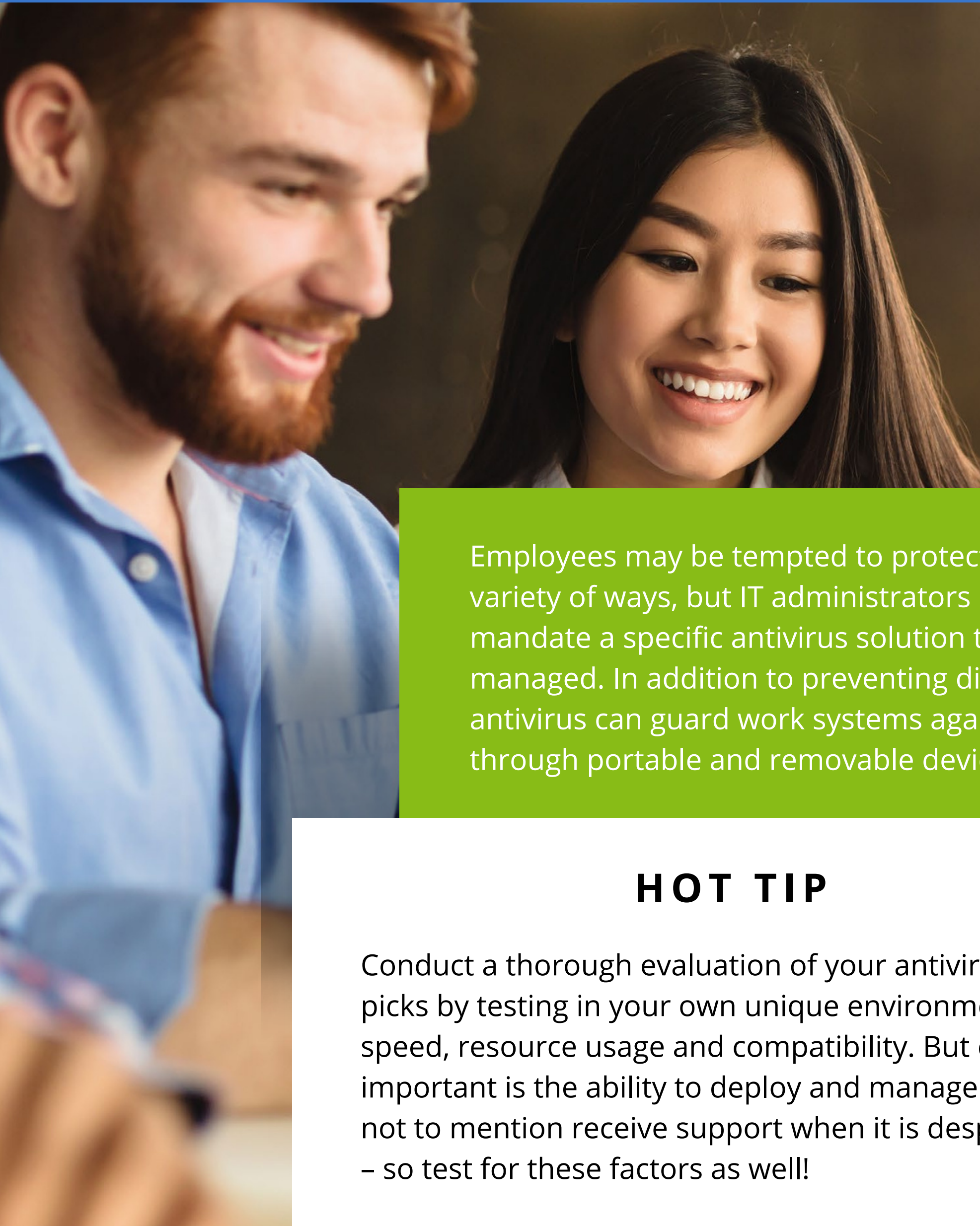
HOT TIP

Establish direct communication channels (dedicated email, phone line, etc) for remote workers to obtain emergency technical support and to report issues. **Build a reaction plan** to restore data and functionality following a data-loss event so that nothing is left up to question.



ANTIVIRUS

6



Employees may be tempted to protect their home systems in a variety of ways, but IT administrators must standardize upon and mandate a specific antivirus solution that can be centrally managed. In addition to preventing different forms of malware, antivirus can guard work systems against threats that arrive through portable and removable devices that employees use.

HOT TIP

Conduct a thorough evaluation of your antivirus shortlisted picks by testing in your own unique environment to gauge speed, resource usage and compatibility. But equally important is the ability to deploy and manage the product, not to mention receive support when it is desperately needed – so test for these factors as well!

BACKUP

7

In addition to their cell phone, remote employees will often use a company issued (or even personal) laptop computer along with USB sticks, external drives, etc. This places critical business data in a variety of locations for a remote employee. Allowing individual employees to deploy and manage their own backup solution is almost certainly asking for trouble.

A solution that includes central monitoring, like **NovaBACKUP**, lets a SysAdmin check backup status from anywhere.

HOT TIP

Backup jobs can be automated to run silently and capture the remote worker's daily data changes and store them on a dedicated server or even in a cloud location like [NovaBACKUP Cloud](#), Microsoft OneDrive, or Azure. With [Central Management Console](#) checking backup status from anywhere a snap.

EDUCATION

8

With remote workers, communication is paramount. Employees must have a deep understanding of how their behavior at home can drastically influence data security throughout the company. Provide education that shows what common security threats look like in real world scenarios. Explain how threats gain a foothold into their system and spread through the company network.

HOT TIP

Working with an outside team for penetration testing offers the benefit of exposing vulnerabilities that the IT team alone would have never considered. Let employees know that simulations will be conducted regularly to assess the company-wide response to modern threats.

Advances in social engineering hacks and deepfake technologies can dupe even the savviest of employees.


WORK FROM HOME SECURITY


In a modern environment with dispersed workforce, protecting employees from threats like ransomware and data breach takes a little planning. Putting a comprehensive strategy in place not only creates physical security, but can also create a long term, positive mental shift that directly affects remote worker habits.



WWW.NOVABACKUP.COM

Speak with our US-based security experts today for a free backup health-check.

 NovaBACKUP Corporation
29209 Canwood Street
Agoura Hills, California
91301

 Tel.: (805) 579-6700
Fax: (805) 579-6710

 Email: ols@novabackup.com
 www.novabackup.com