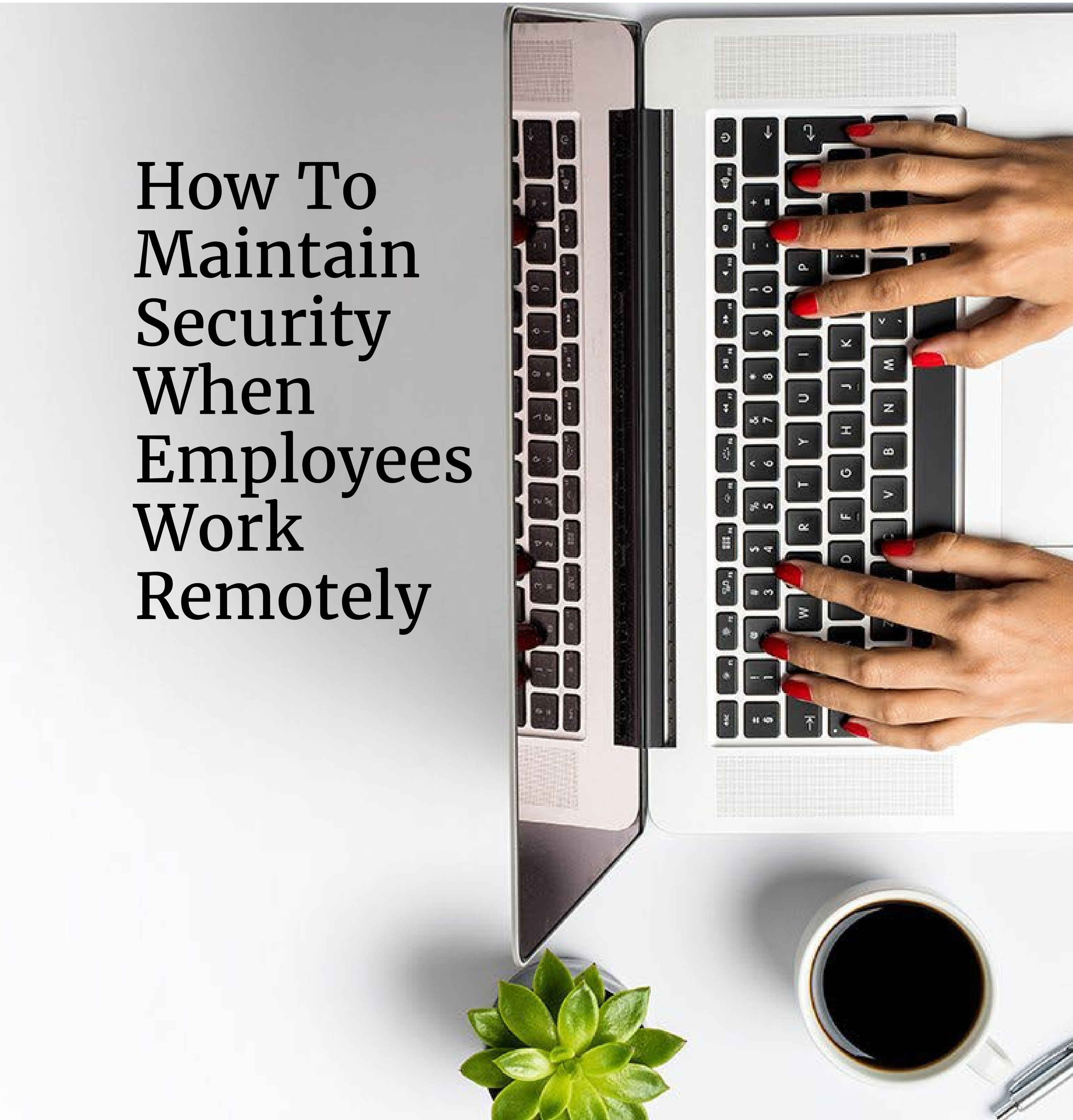
BULLETPROOF
a GLI company

How To Maintain Security When Employees Work Remotely



A lot changed in early 2020. The largest public health crisis of our life thus far began in late January, when the COVID-19 global pandemic reached Canada. By mid-March, states of emergency were declared in most provinces. Businesses fortunate enough to be able were scrambling to sort out how to manage a sudden shift to remote work for an entire workforce in days or weeks, not the months or years their long-term planning may have anticipated.

Plans—and mistakes—were hastily made. Ad-hoc solutions were implemented. IT departments, if they existed, were stretched far beyond their limits. In the background roared social and economic chaos.

It may be hard to feel hopeful. Still, there is much that Canadian businesses can do to meet this challenge and stay prepared for the challenges ahead.

Remote work has been on the rise for well over a decade. A 2018 survey conducted by job search site Indeed found that 62% of Canadian companies offered employees an option to work remotely, and Global Workplace Analytics says that regular remote work in the U.S. has increased by 173% since 2005.

March and April 2020 proved to be a critical test of Canadian companies' remote work infrastructure, and the test continues as COVID-19 forces more businesses to find alternatives to keeping their workforce in the office. Even those organizations with pre-existing remote work options weren't necessarily prepared to move their entire workforce offsite in a matter of weeks (or even days).

As the dust settles and businesses start to adapt to the "new normal", many are realizing that simply making remote work possible was just a first step toward a long-term remote-work strategy. Getting workers out of the office helps keep our workforce safe. Now that your people are protected, it's time to ensure that your business data is protected, too.

62% of Canadian companies offered employees an option to work remotely in 2018.

For many, it's no longer just an option.

The Threat Of COVID-19 To Your Business Data

COVID-19’s threat to public health is significant. Unfortunately, cybercriminals are already using this global health crisis to their advantage to try to steal sensitive data. They’re counting on cracks in your cybersecurity caused by a hasty retreat to home offices and a patchwork implementation of remote productivity software solutions.

Spear-phishing attacks—attacks that target a specific individual or organization — rose by nearly 700% in March 2020 over the previous month, leading the Canadian Bankers’ Association, the Canada Revenue Agency, and many other organizations to release public warnings about such attacks.

Spear-phishing attacks rose by nearly 700% in March 2020. Most were related to COVID-19.

While COVID-related phishing attacks most often target individuals, the threat to your business data becomes clear when you consider how the lines between personal and work-related digital behaviours have blurred given the new reality of many Canadians who are working from home. Employees using personal laptops under a BYOD strategy may not think twice about opening a potentially fraudulent personal email while logged into work accounts.

Other attackers are taking advantage of the large numbers of employees suddenly forced to operate outside of traditional corporate network perimeters, passing sensitive company data back and forth between unencrypted home WiFi networks on insecure devices. Nearly one in five Canadian businesses was impacted by cyberattacks in 2018 and 2019. Given the new challenges businesses face in 2020, that number is certain to rise. And, more than ever, SMBs can’t afford to absorb the consequences of a data breach.

This Will All Be Over Soon. Why Should We Invest In Change?

The fact is that once COVID-19 is under control, most Canadian business will never go back to the way things were pre-2020. While no one wishes for a global pandemic, it is in times of crisis that we tend to see the fastest evolution in technology. Successful organizations will adapt and grow through these challenges, and may very well realize that remote work—securely enabled—is better for their organization and their employees than requiring everyone to be in the office 100%of the time.

Simply put: it's a mistake to put patchwork solutions in place, hoping that this will all be over soon. It puts your data in grave danger now and ignores that the business landscape has irreversibly changed.

Smart companies will take this opportunity to be forward-thinking and implement future-proof solutions.

How Can Businesses Enable Secure Remote Work?

For remote workers, security and productivity must go hand-in-hand. If remote security policies cause frustration and wasted time for employees, they will simply work around them. Without employee education and participation, even the most robust security methods aren't useful or effective.

Employees working from home (or, as public health restrictions ease, from shared spaces like coffee shops, airports, or libraries) must be able to stay compliant with security policies without interrupting their workflows. Businesses that are serious about maintaining security when employees work remotely must choose productivity software with built-in security, with neither feature treated as an afterthought.

If your security solution treats productivity as an afterthought, your employees will find ways to work around it.

Secure Remote Work Software Checklist

If your business is actively seeking a remote work solution that fosters security and productivity, this checklist may help narrow your search. If you're currently relying on a patchwork of software solutions that leave dangerous gaps in your cyber defences, this checklist can help you identify an all-in-one solution that can deliver productivity and peace-of-mind while eliminating the IT problems you're facing today.

The right secure remote work software solution for forward-thinking businesses will:

- Give you (at least) the basic essentials: email, calendaring, mobile document creation and collaboration, team communication, and file storage and sharing.
- Work from anywhere that your employees choose to work, and from a range of devices for companies with BYOD policies.
- Provide built-in tools for managing and authenticating users, including role-based access control.
- Enable multi-factor authentication for enhanced remote work security.
- Help protect users from phishing and business email compromise (BEC) attacks.
- Help protect users from malware attacks.
- Allow for the implementation of a data loss prevention (DLP) policy that can help monitor the transmission of sensitive information and prevent it from ending up in the wrong hands.
- Give users advanced collaboration tools, including video conferencing, whiteboarding, team chat, direct calling, recording and automated transcription options for meetings, and real-time document co-authoring.
- Provide all of the tools your business needs with a layer of embedded security that doesn't inhibit productivity.

Secure Remote Work Solutions From Microsoft + Bulletproof

Microsoft 365 delivers an advanced productivity platform with built-in security features that can be scaled to your organization's needs. Microsoft 365 can securely power remote workforces of all sizes, from small businesses with limited IT resources to enterprise organizations with thousands of employees.

Microsoft 365 includes*:

- Windows 10 Business
- Office 365, which is comprised of all the cloud-based productivity apps that power businesses across the world: Outlook, Word, Excel, PowerPoint, Publisher, and Access.
- Exchange, which provides intelligent email and calendaring.
- OneDrive, the intelligent file sharing and management app for seamless remote collaboration.
- SharePoint, a mobile intranet that lets users easily build dynamic sites to share resources and content for projects, teams, and departments.
- InTune, an integrated endpoint management platform that takes the risk and headache out of BYOD policies.
- Teams, the collaboration platform that keeps remote workers productive and engaged with video and web conferencing, scheduling assistance, screen sharing, chat, whiteboarding, automatic transcription, and more.

- Advanced threat protection and security features that help stop phishing and ransomware attacks, enable multi-factor authentication and conditional access, and restrict the movement of sensitive data.
- Even more intelligent tools to power both remote and on-site work environments, like Bookings and MileIQ.

*not all features available at all subscription levels

Diving Deeper Into Secure Remote Productivity With Microsoft Teams

Web and video conferencing apps have become more important in 2020 than ever before. In a time when being face-to-face with coworkers and clients is a threat to public health, finding ways to maintain interaction is critical.

Many users of web conferencing tools are finding that solutions that used to work just fine for occasional remote meetings simply aren't cutting it anymore. It's easy to ignore a conferencing tool's shortcomings when you only need it once in a while. When it suddenly becomes your main (or only) method of team communication, those minor annoyances quickly become major problems.

Additionally, users have discovered that some web conferencing apps are putting their cybersecurity at risk.

One app that came under heavy scrutiny was Zoom, which came under fire for allegedly selling off user data to third parties as it saw fit. Zoom rewrote its privacy policy in late March 2020, but didn't stop collecting significant amounts of user data. In early April 2020, security expert Bruce Schneier learned that Zoom for Windows could be exploited to steal users' credentials and that Zoom was secretly displaying social media information to other meeting participants.

Video conferencing is just one of the many features of Microsoft Teams, which eliminates security concerns associated with tools like Zoom. Teams offers chat, calling, meetings, file storage, interconnectivity with the rest of the Microsoft 365 suite, compliance controls, advanced authentication capabilities, and more.

Some features of Teams that are exceptionally useful for remote work environments include a whiteboarding app for real-time brainstorming collaboration, automatic searchable meeting transcriptions, meeting time recommendations based on employee availability, and the ability to co-author files directly within the Teams app. All Teams features are protected by the same security protocols as Microsoft 365.

Business conferencing app downloads rocketed up 90% in March 2020 compared to March 2019.

DID YOU KNOW THAT TEAMS IS INCLUDED WITH YOUR MICROSOFT 365 SUBSCRIPTION?

Over 500,000 companies already use Microsoft Teams to streamline their work, collaborate securely, and work remotely. Find out what Teams can do for you and get a customized roll-out strategy, available via remote delivery.

GET AN EXPERT TEAMS ASSESSMENT

Get Bulletproof Remote Work Security With Bulletproof 365

Ensuring that your Microsoft 365 solution is deployed properly is key to creating a secure and productive remote work environment. Beyond basic deployment, training your employees on how to work securely (in a way that doesn't interfere with their workflows) ensures you'll get the most out of your secure remote work software investment.

Like any smart business investment, deployment of Microsoft 365 isn't a set-it-and-forget-it solution. Your cybersecurity plan must evolve along with the threat landscape—which, as we've seen, can change rapidly in response to significant global events. And, while advanced security features can automate some IT functions, the people who make up your remote workforce will inevitably find themselves in need of IT assistance.

Enter Bulletproof 365, the most comprehensive and secure productivity solution of them all. It's leading-edge security, employee training, and support services from a Microsoft Gold Partner wrapped around Microsoft 365, resulting in the most secure cloud services package for Canadian businesses.

Case Study:
Time + Space Media

Time + Space Media (T+S) is a marketing agency based in Halifax, Nova Scotia. They work with clients and partners across Canada and around the globe in a variety of industries to develop and manage strategic, successful marketing campaigns.

THE BUSINESS CHALLENGES

In 2018, T+S was targeted by phishing emails on an almost weekly basis – ones that appeared more and more legitimate with each attempt. The agency had an internal IT person, but with a growing business, their capacity to manage the volume of day-to-day requests was strained. T+S were early adopters of technology, including Microsoft 365 Cloud solutions. But to get the most out of Office 365, users needed the proper training to use the tools and applications effectively, and they needed technical help and support to quickly answer questions and resolve any issues so that staff could keep working without lengthy disruptions.

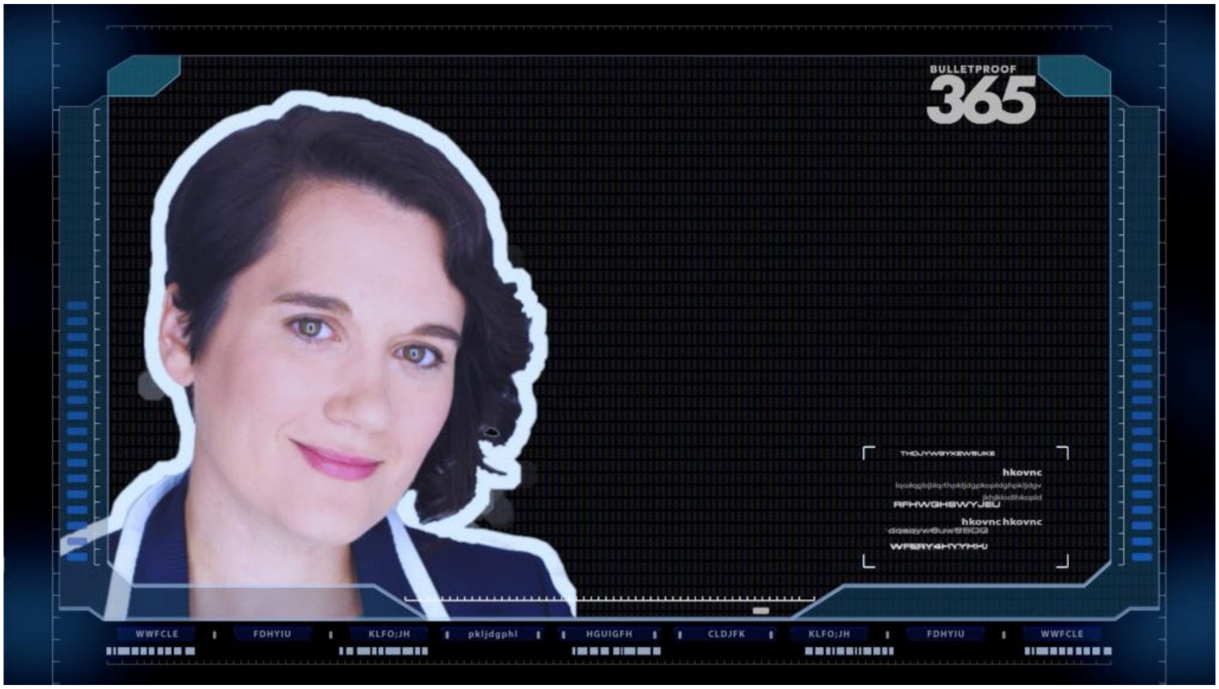
THE SOLUTION

T+S viewed security and cloud productivity as two separate pieces they needed to invest in to solve their business challenges. Bulletproof introduced T+S to a powerful turnkey solution: Bulletproof 365. This product delivered the power of the world's leading productivity platform wrapped in leading-edge cybersecurity, unmatched employee education, and 24 x 7 IT support. Bulletproof 365 was a perfect match for their needs and provided all the pieces to solve their business challenges, including:

- Expert cybersecurity protection.
- 24 x 7 technical support for their users and IT Manager.
- Upgrade to a secure Windows 10 operating environment.
- Employee onboarding and education modules to empower staff and accelerate adoption.
- Security Aware training to educate employees on cybersecurity, transforming them from targets to active defenders of organizational security.
- Seamless integration from configuration to roll-out, making it easy for T+S to manage change.

THE RESULT

Today, with Bulletproof 365 in place, T+S has the protection they needed, the productivity tools and cloud technology they wanted, and the peace of mind they were missing before Bulletproof 365. 24/7 helpdesk support has reduced the load on their IT Manager and significantly shortened response time to user problems or questions. The increased security protocols also helped T+S qualify for the cybersecurity insurance they needed. They now reference Bulletproof 365's security and protection as a selling point in new business RFPs.



Watch the testimonial from Megan Stephens, VP of Finance + Administration at Time + Space

Find A Bulletproof Solution For Secure Remote Work

A lot of IT consultants can set you up with remote work tools, but no company can set you up for success and security better than Bulletproof. With more than 17 years in the security business, it's in our DNA. Protecting your privacy and data is built into everything we do.

Our full-service Microsoft Team has deep experience setting up, customizing, and migrating businesses to the cloud, and our track record is impressive: more than 20 million files and 100,000 users migrated so far. We are proud to be a Microsoft Gold Cloud Partner.

Our security pedigree is second-to-none, protecting more than 70,000 users and networks on six continents. Our 24x7 Service Desk supports over 50,000 users and over 10,000 network devices in more than 300 client offices around the world.

SOME CLOUDS ARE SILVER-LINED. OURS IS KEVLAR.

Download the B365 Brochure to learn more about getting a complete package of managed remote productivity and security tools—including Microsoft 365—for one affordable monthly fee.

DOWNLOAD THE B365 BROCHURE