SIMformation

Understanding VPNs

The move to remote, or "work from home" employees, has created new interest in VPNs, or Virtual Private Networks. Is this something your remote workers would need? The answer is: it depends. We will explain:

To understand how a VPN works and whether you should use one, it is best to first understand what happens when you're using the Internet. Whenever you open up a web browser and go to a website, you're connecting to that website and exchanging information with it. This is your Internet "traffic," and it can reveal quite a bit of information about you, including what websites you visit, your IP address, and more.

A VPN acts like a "tunnel" for your Internet traffic. Your traffic goes into the tunnel, and emerges out of one of the exit nodes of the VPN service. The tunnel encrypts your data, making it undecipherable to your Internet Service Provider (ISP). At best, your ISP can see that some encrypted traffic is going to a VPN service, but not the contents of that traffic, and not where it comes out of.

The interesting thing to note here is that, with this basic functionality, a VPN can actually serve many different needs.

A VPN is any and all of these: [1] a tunnel that sits between your computing device and the Internet, [2] helps you stay anonymous online, preventing surveillance, spying, and excessive data collection of big companies, [3] a tool that encrypts your connection and masks your true IP address with one belonging to your VPN provider, [4] a piece of software or app that lets you access private resources (like company files on your work intranet) or sites that are usually blocked in your country or region.

Without a VPN, your Internet Service Provider, or ISP, can see almost everything you interact with online. Who you connect to, what type of traffic, where you are geographically. Not a comforting thought, especially if you are dealing with confidential company information while in "work from home" mode.

If you use a VPN, your ISP knows you've connected to a VPN, but it cannot inspect the content of your traffic, and does not know where it comes out at the other end. These tools have been in use for businesses for a long time now. They are typically used to access resources remotely as if you were at the office. In some cases there have been performance boosts by using a VPN, because artificial throttling is circumvented by the use of a VPN. Since you are tunneling your connection, your ISP can't peek at your traffic and throttle it, based on the kind of traffic. Some ISPs, for example, throttle users' traffic when they see file sharing.

A VPN can be established either through hardware or software. Most remote workers probably do not have the more robust router needed for setting up a VPN, plus some ISPs that provide the router for their service discourage this practice. Thus, a software solution from a third-party provider is often the first choice for at-home workers. This application will provide VPN tunneling to the computer it is installed on, and only that, so keep that in mind, so if you bounce between a laptop and desktop PC from home, consider which is best for your business work.

You should have a VPN provider that doesn't discriminate the type of traffic that flows through their network. Some smaller VPNs don't have the necessary infrastructure to handle large volumes of Peer-to-peer or bittorrent traffic, and either ban it outright or have actual data caps.

Another factor that makes a VPN really perform is when they have a lot of exit nodes. These exit nodes are locations that can be used to circumvent geolocation. The more that are available, and the greater the variety, the more versatile and useful the VPN service is.

Remember, when you're thinking about adopting one of these tools, you're transferring trust: When you use a VPN you transfer access to your traffic to a 3rd party, the VPN provider. All that visibility that users balk at relinquishing to their ISP has now been handed over to their VPN provider. Careful consideration should be given to the trustworthiness of said VPN provider. VPNs should not be viewed as shadowy tools. They are, in all actuality, business and privacy tools. They let employees connect to company resources away from the office—which is of the utmost importance today. And they allow you, the user, to reclaim a measure of privacy.

SIM2K can help you with establishing VPN connections for your remote employees, and for any other business purpose you require, such as connecting directly to a vendor or financial partner where security is necessary. Please contact us for more information on VPNs and how we can set them up for your business.

SIMformation

Our Changing World

Crisis brings opportunity in different ways. The Covid-19 pandemic has pushed many businesses to shutter the traditional office and employees are now "remote workers" connecting to company resources from home.

We discuss the need for secure connections for computers on page 1 with our VPN story. But access to company data and documents is only one fraction of the business story. There has been a rise in the use of platforms like Microsoft Team, or Zoom, or even Facebook, to link employees and have what used to be a conference room discussion.

But your company identity goes further than your employees. You have a phone number, and what has happened with the office shut down during the pandemic? Is there one lonely employee delegated to phone duty on hand to answer calls? And what happens to these callers – do they get to speak to someone or end up in voice mail and hope they get a return call.

This is where having a unified communications system comes into play. SIM2K is a Zulty partner, and sells a robust communications system that offers great flexibility in times like this. From the ability to direct calls to different numbers, or even the ability to download an app from the Apple App Store or Google Play Store that transforms your cell phone into your office extension, Zultys has solutions to keep your business phone system up and running and callers will never know whether your employees are office-bound or working from their dining room table.

For example, as mentioned, the ability to download the Zultys Mobile app turns your personal smartphone into your office phone. You log into your Zultys server, and at that point, all calls to your office can come to your phone. And, when you place calls, the person at the other end sees your office number on Caller ID, not your personal cell phone number. Plus, the mobile app brings along all the calling features you'd find at the office, such as your directory of contacts, call log of made/received/missed calls, a record of all voicemails with playback ability, and instant contact with other employees by dialing their extension - you no longer need to know their personal or home phone.

The Zultys systems that SIM2K provisions are offered in three ways — an on-premise server that handles all communications functions; as a software package that is loaded on your existing server to provide the system; or as a Cloud-based service where you no longer have any hardware (other than the phones themselves) to install and maintain. Each option has their own pluses and minuses, based on your business calling needs, so we will sit down with you to determine which way would be best for your company.

And, rest assured, as a Zultys partner our services do not end with the sale. We provide training for your staff, we do software updates on your behalf where applicable, and our Support Team is there to trouble-shoot problems, add functions and otherwise assist just like we do for computer networks.

So if your company is considering extending the remote workplace even as restrictions ease, if you do not have a unified communications system in place, please call SIM2K and we will discuss how we can bring the power of Zultys to your office.

Chrome Commands Browser Market

Google's Chrome cracked 70% last month in browser share, setting another record as it reached a number held by only two other browsers in the history of the web. According to data from Net Applications, Chrome's share during June rose four-tenths of a percentage point to 70.2%. The browser has been on a sixth-month run, adding 3.6 percentage points to its account since January.

More notable was that, by breaking the 70% bar, Chrome became only the third browser to reach such a dominant position, following Netscape Navigator (ancestor of Firefox) in the 1990s and Microsoft's Internet Explorer in the first decade of this century.

Chrome's continued climb may not be sustainable over the long run – that would require the extinction of at least one rival – but on a strictly linear basis, the browser's future looks rosy. IT experts forecast that on a 12-month average change in share, Chrome will hit 71% by September and beyond 72% by year's end. Microsoft's Edge will be the sole conceivable threat to Chrome's overwhelming majority, and then only if organizations – businesses and universities in particular – adopt the Chromium-based clone because of its manageability and then users mimic that at-work move on their personal devices after hours.

Microsoft's two browsers, Edge and IE, combined to post a rare increase in share, upping their combined number one-tenth of a percentage point in June to 12.6%. The growth was all on Edge, which gained two-tenths of a point to reach 8.1%, a record for the five-year-old browser. Meanwhile, IE lost half as much, slipping another tenth of a point to 4.5%.

Things are looking up for Mozilla as June was the third straight month that Firefox held onto or increased its share; the browser ended June at 7.6%, up four-tenths of a point from its April and May 7.2%. At the end of June, Firefox's share was identical to its end-of-February total. Even with the increase, Firefox remained in third place behind Edge. (Firefox lost its long-held second spot in March.) The gap between the two shrunk by a tenth of a point to five-tenths of a percentage point.

Finally, Apple's Safari shed three-tenths of a point, dropping to 3.6%, its lowest mark since October 2019.

Many Windows 10 machines are now being automatically updated to Chromium Edge (see story on next page). If you do not wish to have your company's PCs updated to this new version, contact SIM2K about installing the blocker kit that will undo the automatic download and installation.

Why Covid-19 Tracking Apps Won't Work

To help track people who've been exposed to COVID-19, technology companies and governments have proposed contact tracing apps as a solution. Such apps would add a tech element to something health care workers have done manually for decades, where they've thoroughly interviewed people to get a history of who those people may've exposed to infection. But some of the same tools that have fueled mistrust in big tech are what the industry is proposing as part of the answer. Critics warn that the whole effort could fail if the tech industry can't pull itself out of the hole its own missteps dug over the years.

But, to date, contact tracing apps have turned out to be a huge waste of time and money. Hundreds of governments and health organizations around the world have scrambled to get contact tracing apps to the public. But the apps are disappointing everyone.

Here are the main reasons experts say tracking won't work:
1. It can't work without frequent and universal testing.
2. It doesn't address all the ways people get the virus.
3. It doesn't notify beyond one level of contact.
4. It's not universal.

On a call to (to IT writers) explaining how their contact-tracing capabilities would take on the COVID-19 pandemic, representatives from Google and Apple laid out their biggest challenge: getting people comfortable enough to actually use the technology. The whole project would fail if they couldn't convince enough people to sign up.

To do that, Apple, Google and any government looking to take advantage of a contact-tracing app have to climb a mountain of skepticism, created in part by the tech industry's long history of data abuses. For years, lawmakers, privacy watchdogs and regulators have felt deceived by tech companies, who've used technical details to hide their tracking capabilities.

The "move fast and break things" mindset has created innovations, but it's also deeply broken public trust in big tech. Facebook's mission of "bringing the world closer together" also helps it gather millions of people's information for targeted advertising. Google offers educational tools, and directions through its Maps services, but it also faces lawsuits for location-data tracking and allegedly collecting students' biometric data. Apple, which has turned privacy into a feature of its products, has previously taken shots at its rivals for their tendency to share their users' information.

The tech giants want to improve on the concept of manual contact tracing by using Bluetooth technology to log exposures rather than relying on a person's memory. Apple and Google's concept looks to use randomly generated IDs on devices that silently send out Bluetooth signals to other devices that have the app installed.

If people mark themselves as COVID-19 positive, and give consent to share that information through the app, then every device that interacts with those people's ID in a select time range would get a notification about potential exposure to the disease.

Governments in the US, the UK and Singapore have warmed to this concept, but for any of this to actually work, you need people to download the technology. And government officials rolling out this tool have found that especially challenging.

"Random Tid-Bytes"

Microsoft Closes Retail Stores

Microsoft said it would close its chain of retail store and take a $450 million charge against earnings to account for the permanent shutterings. The stores – Microsoft had 82 worldwide, all but 10 of them located in the U.S. – have been padlocked since mid-March, when the Redmond, Wash. company closed them because of the coronavirus pandemic. None had reopened before Microsoft slid them into the "really dead" category. In lieu of the closed-for-good retail stores, Microsoft will expand its online efforts, the company said, although it characterized the move as a "new approach to retail," which makes little sense since it will have no retail beyond microsoft.com and XBox systems. To put the "happy face" on this announcement, Microsoft said "Our sales have grown online as our product portfolio has evolved to largely digital offerings, and our talented team has proven success serving customers beyond any physical location." The charge against earnings will be taken in the June quarter, which also ends Microsoft's 2020 financial year, the company said.

Scam of the Week: Survey Says… It's a Scam

Some retailers use online surveys to learn more about their customers. Completed surveys are often rewarded with small consolations, like a coupon. Sounds fun, right? The bad guys sure think so! Scammers are posing as well-known brands and sending emails that advertise extravagant rewards, like a new iPhone, for just a few minutes of your time. Typically, the survey website displays a message claiming that there are only a small number of rewards remaining – this creates a sense of urgency to complete the survey. Usually, at the end of the survey, you're told that you have won the prize and all that you have to do is pay for delivery. Of course, you didn't actually win anything. The fake prize and request for your shipping details are just an excuse to gather your name, address, and payment information. For your protection, follow these tips when you are answering retailer surveys:
- Always question a sense of urgency. Real companies want real results. If a survey is urging you to hurry, it's because they want to get to the part where you hand over your personal information.
- Legitimate retail surveys clearly outline the rules from the very beginning. If you're suddenly asked for payment or other unexpected information, it's a scam.
- If it sounds too good to be true, it is! As lovely as it would be, no one hands out free iPhones (or other extravagant rewards) over the Internet.

Updates to Chromium Edge Coming

Microsoft has warned enterprise and education customers running Windows 10 that it will start replacing the old, original Edge browser on their PCs with the newer Chromium-based version on or after July 30. According to Microsoft, PCs serviced by Windows Update will be automatically upgraded to the Chromium Edge. First to get the forced swap will be machines in educational settings, Microsoft said, citing back-to-school scheduling for the prioritization. Organizations that want to stymie this effort can use the Blocker Toolkit for Edge-to-Edge released in December 2019 and available for download on-line. The kit blocks Windows Update delivery of the new Edge, but it does not prevent students or workers from manually obtaining the Chromium-based Edge.

Lessons IT has Learned from the Covid-19 Crisis

The coronavirus pandemic has had a jarring impact on virtually every facet of life and business — including IT. As lockdowns end and many businesses begin to reopen, at least on a limited basis, technology executives are looking for a return to some semblance of normalcy.

For sure, the worldwide health crisis has dramatically changed the way IT departments provide services to their organizations. That includes supporting the massive shift to a work-from-home model that few could have fathomed a few months ago.

As with any other event on this scale, there are lessons to be learned. Here are some of those, shared by IT leaders and other experts.

Organizational agility begins with culture

The past few months have reminded IT leaders that change is inevitable, and that culture plays a big role in adapting to change. This mentality includes focusing on the value IT is providing for each customer, embracing change, asking "why" questions, and thinking and acting like a small company, among other things.

Remote work is now a fact of life — and supporting it requires structure

Prior to the pandemic, many enterprises were experiencing a rise in the remote workforce, thanks in large part to increased use of mobile technology and the cloud. The health crisis made working from home the norm, and for many companies the shift might be long term if not permanent.

"One of the biggest lessons I've learned from the pandemic is about the need for leaders to establish a structure for working remote, including encouraging team members to set and indicate working hours in their calendaring systems, and then re-setting project timelines and help desk coverage times to accommodate this new availability matrix," says one CEO. "Without this structure, employees tend to continue to operate in 'emergency' mode, feeling the need to be available 24x7."

The mission of the CIO has now been expanded to enable employees to be productive in their home environment. "When we first went remote, we saw an initial decrease in productivity due to everyone getting adjusted," the same CEO discussed. "But now that our employees are set up for success at home, we've actually seen an increase in productivity by 8%. We've learned that our employees will work hard no matter where they are, as long as we're providing the tools and resources for them to thrive."

The cloud and virtualization have become even more critical

Clearly cloud services have been taking on an increasingly important role at organizations over the past few years. But the pandemic raised the level of urgency to a new level, as companies scrambled to support legions of home workers, roll out and maintain collaboration tools, and more easily deliver applications, capacity, and storage to a far-flung workforce. One company said their reliance on the Cloud allowed them to quickly enable over 90% of their employees to work from home during the first week of pandemic. After migrating to Microsoft Office 365 two years ago this company also implemented the Microsoft Teams collaboration tool, which enabled it to swiftly send its workforce home without missing a beat in productivity. For them, the cloud has helped accelerate the adoption of advanced technology across the organization.

Organizations need flexible software platforms and strategies

IT teams didn't have a lot of time to prepare for the monumental changes caused by the pandemic, so having a set of software platforms in place that could be quickly implemented and scaled to support operations was vital. This is critical for two reasons – first, it's important to be able to quickly implement functionality. Second it allows IT execs to distribute the overall workload among application staff so that one group was not totally overwhelmed.

Simplification and standardization are vital

Oftentimes the less complexity there is with IT, the better. That can certainly be the case in an emergency situation like the pandemic. Many companies reported that their investments in simplifying and standardizing had been essential to their ability to successfully and quickly transition employees to working from home.

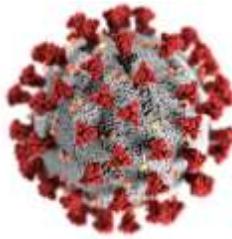### A people-centric approach to IT security is necessary

Remote workers tend to abandon security procedures that interfere with their workflow and productivity, and as a result are often willing to bypass data protection checks if they can. However, hackers are increasingly targeting remote workers, and it's vital that these employees be able to work productively without being hindered by security processes.

To prevent remote workers from taking security shortcuts, IT teams need to balance security with user experience and productivity. IT teams must provide a streamlined and hassle-free work experience while building transparent cybersecurity controls.

AI and machine learning can be game-changers

Even before the pandemic, many enterprises were grasping the potential of AI and machine learning (ML) tools as a way to draw unprecedented value from data and improve processes. For companies in industries such as healthcare, the technologies quickly opened new opportunities to advance data management.

Given these lessons, one positive message that can be taken away from the pandemic is that it has opened up the eyes of many on what technology can do and how it can help improve employees' ability to complete our work. Going forward, IT experts feel that they now have people who understand the benefits of technology and will start to demand innovations. As your company's workflow may be forced to adapt to these new conditions, SIM2K has a variety of solutions that can be brought to bear to help you continue to stay productive during unique times. Call us for more information on solutions such as these.