February 2022

TechTidbit.com

brought to you by Tech Experts

The Security Problem Of John's "Other" Laptop

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Love it or hate it, Working From Home is huge and here to stay.

As a nation, we've really embraced the changes forced upon us by the pandemic. Many businesses have become more flexible with a mixture of office-based workers, hybrid workers and fully remote workers.

We had no idea that we could change so much, so quickly, did we? Work just doesn't look the same as it did in 2019.

And because of that, cyber security in 2022 doesn't look the same either. When you have people working away from your office, you need to take additional security measures to keep your data safe.

Even before we'd heard the word "Coronavirus," many of us were working from home now and then. Checking emails on the weekend. Finishing up a project in the evening. Getting a head start on your week.

Now, Working From Home has to be taken more seriously. If any of your staff works anywhere away from the office, there's a chance they're taking unnecessary risks with your data.

Many businesses seem to have this covered. They've invested in new company devices, increased remote security, and have trained their people on best practices.

But there's something important some businesses haven't considered: unmanaged devices.

We mean devices used to access business data that the company doesn't know about. Your company laptop and mobile are likely to be safe because they've been set up properly with managed security.

But what about other devices your team use for work? John's "other" laptop, the one he grabs sometimes in the evenings just to do his email.

In fact, the risk is bigger than this. There's a risk from virtually all other devices on your team's home networks.

Their games consoles, other laptops, tablets, and phones. Most people have an entire household of gadgets connected to the network.

And almost all of them are at risk of being accessed by cyber criminals.

The bad guys will find a way

The big thing we know about cyber criminals is that they're very persistent. If they want in, they will keep going until they find a way. And sometimes, your team will make it too easy for them.

All a hacker needs to do is access one device on someone's home network. Let's say it's a games console. Once they access the console, it's a waiting game. The hacker will be patient and watch the traffic on the network. It's possible they'll be able to learn enough from that to eventually spot a security hole with a work device.

Often, by the time someone's noticed something's wrong, it's too late. The hacker may have gained access to the VPN – the Virtual Private Network that allows you to securely connect to the business's data.

And that means they can potentially gain access to your business's valuable data. They might make a copy and sell it on the dark web.

Or they might install malware, malicious software that can do damage and corrupt data.

Or the very worst case scenario is they launch a ransomware attack, where your data is encrypted and useless to you unless you pay a huge ransom fee.

This is the scariest thing that can

Continued on page 4

Your company laptop and mobile are likely to be safe because they've been set up properly with managed security. But what about other devices your team use for work? John's "other" laptop, the one he grabs sometimes in the evenings just to do his email.

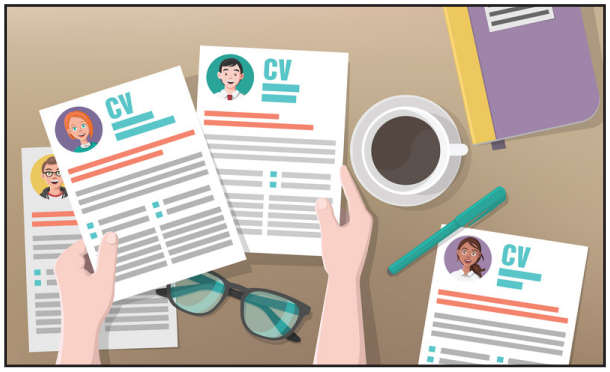
How To Hire Top Talent With Advanced Tools

"These AI-based tools will resolve the conscious and unconscious bias in the sourcing and screening process. These tools do not consider the candidates' demographics such as age, gender, and race. Rather, they focus on hiring based on talent and skills."

Setting up the best recruitment tool can solve numerous business related problems. A major problem that almost every business encounters is hiring a qualified candidate.

According to a survey, 87% of HR professionals reported that they could not fill positions with eligible and qualified candidates.

Apart from that, many companies find it difficult to reach qualified candidates, provide a remarkable candidate experience, and maintain diversification in the workspace.



You can solve these problems and numerous others by incorporating a top recruitment tool in your human resource department. Below, you will learn some benefits of using the tools for an effective hiring process.

Online recruitment tools increase recruiters' productivity. By shifting to advanced technology, your team will learn new methods and factors to identify the best talent.

These tools are a huge help for them to reach new people through social media. Hiring the best candidate from a long list is an arduous task. However, you can automate your tasks using a recruitment tool, thereby saving precious time and effort.

While hunting down potential candidates, communication is really important. Using recruitment tools, you can maintain efficient and time-saving communication channels, effectively keeping applicants in the loop.

Recruiting tools you should use

The hiring process is no longer a manual task for most businesses. The reason top businesses are leading in this dense and competitive environment is that they focus more on hiring the right talent.

With manual hiring, the partiality in the process has a great impact on final decisions. Even if they try not to bring their emotions into the hiring process, they make mistakes.

Therefore, it is the right time to switch to advanced recruitment tools and enhance the skills of your human resource team. Here are some popular options among top businesses:

Recruitment chatbots

Going through an interview, candidates are more comfortable communicating with an AI tool than a team member. By knowing they must communicate with the chatbots, they will be confident inbeing transparent.

With recruitment chatbots, you can schedule interviews or take tests online. AI chatbots for recruitment not only help you make better decisions but provide an amazing experience to the candidate.

AI for screening

The screening process provides essential information about candidates and compares the top applications among all. Depending on the number of applications, this process is time-consuming.

Moreover, screening hundreds of profiles of applicants will be discouraging for your employees. While reviewing applications, they might overlook things due to pressure. However, you can automate your screening process through artificial intelligence recruiting tools.

These tools will shortlist eligible candidates, effectively reducing time and cost per hire.

Reducing bias software

Recruiting teams who use artificial intelligence to recognize talent can reduce the bias from screening, sourcing, and job descriptions. These AI-based tools will resolve the conscious and unconscious bias in the sourcing and screening process. These tools do not consider the candidates' demographics such as age, gender, and race. Rather, they focus on hiring based on talent and skills. Reducing bias from the workplace will prevail in bringing diversity among the candidates.

Traditional techniques for recruiting talent include posting ads in newspapers, and placing boards. To speed up the hiring process and recruit the best talent, integrate advanced tools in your recruitment department to attract better quality candidates.

Three Ways To Evaluate Employee Performance

A performance management system enables you to evaluate your employees and helps you bring transparency to the process. These tools facilitate you with features for engagment and accountability of your employees across the company.

Factorial is a performance management tool that enables you to track the progress of each employee. This tool helps you customize the questionnaires and assign reviewers to easily manage and evaluate your teams.

With this tool, you can generate custom reports, create employees' portals, add features in the individual portal and send a notification to the participants. You can access this software through a browser and your phone.

You can also use Factorial to integrate different add-ons and third-party plug-ins to streamline your workflow. You can unlock numerous connector tools with Factorial if you have an account on Zapier. The tools you can integrate include Google Calendar, Slack, Gmail, and Outlook.

Initially, they offer you a 14-day free trial that helps you assess the application. This management tool includes a few limitations that might slow you down a bit.

Trakstar is a highly customized tool to assess the performance of your employees. This tool includes comprehensive features and offers detailed analysis.

The interface of this platform is user-friendly and easy to understand. The developers designed this tool according to advanced social media websites so everyone can get the hang of it.

The top features that this software includes are 360-degree/ multi-rater feedback, employee engagement surveys, and task management for thousands of employees.

It also facilitates you with setting SMART goals, customizes appraisal forms, and creates a flexible workflow according to the organization's needs.

SAP is a popular and user-friendly tool that enables you to develop and retain employees, reduce attrition, optimize benefits, drive engagement, and increase the productivity of your employees.

This intelligent tool includes RPA or AI and robotic process automation capabilities. Furthermore, you can perform embedded analytics. SAP is an expert-recommended feature that offers flexibility to your employee management.

You can customize the SAP ERP based on your business infrastructure to perform wide-ranging tasks and activities. It offers you an SAP API business hub that includes digital content packages with sample applications and APIs.

This platform offers you a 30-day free trial period. After the trial period, they will charge you every month depending on the number of users.

"A performance management system enables you to evaluate your employees and helps you bring transparency to the process. These tools facilitate you with features for engagment and accountability of your employees across the company."

Tools To Improve Internal Communication In Your Business

Improved internal communication will build stronger teams, increase employee engagement, and enhance productivity.

You can build a better and friendly workplace by increasing communication between employees.

However, the main challenge is to implement an internal communication tool into your business system. Choosing the best tool among all is a difficult decision to make. Therefore you can choose among these top tools for internal communication:

Intranet is a centralized communication tool to share, gather, and access information. This is a private network that requires a web connection.

Digital Signage is a workplace communication tool that requires strategically placing screens. You can also use instant messaging applications dedicated to internal communication such as WhatsApp, Facebook, Skype, etc.

After implementing the tool into your workplace, ask your employees to share all information through the channel. Then, create a team or assign managers to lead the communication process.

A communication team is better than a meeting, and you can utilize it in numerous ways, including training sessions and surveys.

The Security Problem Of John's "Other" Laptop, continued

happen to your business's data. You do not want to risk this.

What's the solution?

The answer isn't straightforward. Unless your business wants to take on the security responsibility of all of your staff's home networks and all of their devices too. It's just not realistic.

However, there are things you can do to lower your risk of an intruder getting into your business network via an unsecured home network. And it all comes down to a layered approach to security.

There are four things we recommend.

Help your team secure their home routers

The router is the box that spreads the Internet around the house. You might know it as the Wi-Fi box.

You can give every member of your team advice and direct support in keeping their router secure, such as changing default admin passwords to randomly generated long passwords, help them make sure the router's operating system, known as firmware, is always up-to-date.

And disable remote access, so no one can change anything in the router unless they are physically in the property.

You could also create a policy to make it clear your team must follow standard security guidance for their home network if they want to Work From Home.

Make sure your systems are monitored

Your IT support partner should be monitoring your systems. That doesn't mean having a quick check that everything is working as it should be and waiting for you to flag up any issues.

It means they should be constantly monitoring your network 24/7, looking for anything unusual that may cause an issue, and preventing problems from escalating.

Unfortunately, cyber criminals don't work to our schedules. They certainly don't work a 9-5 job. It's more likely that they'll make changes when they believe no one is watching.

And they may launch an attack at 3AM on a Sunday morning to give them as much time as possible to do what they need to do. Your IT team needs to be ready.

Reassess your VPN

Virtual Private Networks have been invaluable over the last couple of years, but while they've allowed remote access to your business network, the large-scale use of VPNs has created a higher risk of a data breach.

If a hacker breached a device using a VPN to get onto your network, it means they could have full access to everything… without needing to pass further security measures.

That's scary.

An alternative option is to ditch the VPN and take a zero-trust approach. This means the credentials of every device and person trying to access the network are challenged and must be confirmed.

If a hacker does gain access, they can only cause damage to the specific system they have accessed.

Carry out a security audit

The best way to ensure your business is protected from this kind of attack is to get a security audit.

Take a look at the security you already have in place and identify what's missing to keep your business as safe as possible without getting in the way of everyday work.

If you're working with an IT support provider, they should already have a fully detailed account of your security systems.

It's worth asking them what weak areas they have identified and your options for improving them.

An expert will be able to assess your business and the way your people work and make suggestions on the security measures that will work best for you.

Create new service requests, check ticket status, and review invoices in our client portal: http://www.TechSupportRequest.com

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com