



Newsletter

What's Inside

Guidelines on monitoring your employees' online activities

Page 01

How to avoid getting hacked by Cybercriminals and protect everything you've worked so hard to achieve

Page 02

Featured Partner: DUO

Page 03

The Cloud: Connecting us during the COVID-19 outbreak

Page 04

Guidelines on monitoring your employees' online activities

THE CASE FOR MONITORING

Here are several reasons why monitoring your employees' activities on company devices is a good idea. It can help you:

- Protect your organization from data theft or harm – because careless or disgruntled employees may leak or steal your data.
- Ensure you have a harassment-free workplace – because cyberharassment (sexual or otherwise) happens among employees.
- Ensure members of your staff comply with policies – such as not downloading illegal programs or spending time on websites with illegal or hostile content.
- Provide evidence in case of a lawsuit – should an employee participate in illegal activities using your business's computers (heaven forbid!), monitoring their device can provide evidence of their involvement.

ARGUMENTS AGAINST EMPLOYEE MONITORING

Of course, you should also be aware of the potential downsides to monitoring. These include:

- Productivity loss – monitoring can put a damper on employee morale, and you may see the distrust leading to productivity losses.
- Lost privacy and lawsuits – you'll likely learn personal details about your employees that you would've never known about had you not monitored them. You may discover their political or religious views, sexual orientation, or medical problems. This subjects your business to potential privacy or discrimination issues if you or your management team acts negatively based on any of this information.

MONITORING GUIDELINES TO FOLLOW

If you decide to monitor your employees, here are a few tips you should follow.

1. Create written policies

When you monitor your employees, ask yourself: "Am I doing this for security purposes? Is it to ensure my employees aren't wasting time on games or social media?" If your monitoring policies are too strict, you could create an atmosphere of distrust.

2. Tell your employees

It's important to inform your employees about the scope of your monitoring policies. If they find out you're doing it secretly, you could face legal issues. By being transparent, you may actually see a boost in productivity by deterring employees from wasting time on the web.

3. Get the right technology tools

You don't need to know each and every employee activity, so look for apps and software that alert you of the most relevant problems, so you can focus on more important tasks.

If implemented correctly, employee monitoring makes your business more secure and productive. For more information about security and other IT support tools, [get in touch with us today.](#)

Contact RJ2
(847) 303-1194

Corporate Office
1900 East Golf Rd.
Suite 600
Schaumburg, IL 60173

Chicago Office
333 S. Wabash Ave
Suite 2700
Chicago, IL 60604

How to avoid getting hacked by Cybercriminals and protect everything you've worked so hard to achieve

Cybercriminals are always looking for new ways to steal data and make a buck at the expense of someone they've never met. They don't care if they ruin someone's life or destroy a business in the process. This is why it's so important to stay up-to-date with the latest technology.

Cyber security threats are constantly evolving. If you let your software or hardware – or both – fall behind the times, then you put your business at serious risk. Five years ago, your malware protection might have been the best on the market. If you haven't updated since then, you need to change that. Here's what you can do right now to protect everything you've worked so hard to achieve.

Stay updated. After a while, developers and manufacturers stop supporting their old hardware and software. Many of them simply don't have the resources to keep updating older products. They need to make sure their current products are supported and secure. After five years, they may stop sending out security patches for their software. Or they might not offer help-desk support for a seven-year-old router.

If you run into this situation, you may need to invest in new equipment or software. It can be a tough pill to swallow, but it doesn't compare to the cost of dealing with a hack or data loss. Data loss can be devastating for a business. Some never recover and have to close their doors because the cost is so high – and customers don't want to give their money to a business that isn't going to keep their data secure.

At the same time, you need to update your existing equipment and software. Make sure everything has the latest security patches. Most hardware and software come with an option for automatic updates. If you're concerned that you'll miss an update, then keep this option on. It is a good idea, however, to check everything periodically to make sure the updates are being applied, just in case.

Say yes to proactive monitoring.

Proactive network monitoring can be your best friend in the fight against cyber-attacks. Many IT security firms now offer proactive services. Basically, they watch your network 24/7. If a threat is found, they can

stop it before it does any damage. They act immediately to stop those threats.

You can sign up for real-time reports or just get updates once a week to stay informed so you know what's going on with your network. Proactive monitoring can also make sure your systems are up-to-date (coming back to our first point). If they detect a vulnerability, then they can work to patch it. This means you have so much less to worry about so you can focus on what really matters: growing your business and taking care of customers!

Back up everything.

If you don't have data backups for your business, it's time to change that. Setting up a data backup system – whether it's local or cloud-based – can sound like a lot of work. You might have a ton of data, especially if you've been in operation for long. But not having a backup system can tear your business apart.

If a piece of hardware fails or a hacker gets into your data, you may have to dig deep into your pocket to recover it or you may just lose it all. There are a lot of scenarios where data can be lost.

Investing in a backup system, like a secure cloud backup, solves this. You can set up a secure system that backs up data daily (or nightly), weekly or whenever you need it. It's good to keep backups off-site just in case anything happens on-site (electrical surges, flood, fire, theft, etc.). If data is lost or your network falls victim to ransomware, then you can restore your data and continue operations!

These tips can seem like a lot, but when you partner with a dedicated IT services company, you can overcome a lot of hurdles. Working with IT specialists is how to keep your business safe in a world where cybercriminals are actively trying to break in. You want someone with the expertise to secure your network watching over your shoulders.

RJ2 SPOTLIGHT

Megan Muzzillo

Support Admin

Megan has been working in customer service for 4 years. Before joining the RJ2 family, she worked at Lifetime Fitness, where she gained experience and worked in higher management roles for multiple departments, including account management and customer service. She is currently enrolled in school to finish her degree in Business Management.

Megan joined RJ2 Technologies full time in October of 2019. She holds the role of Support Specialist in the Administration Department.

Fun Fact: Megan was a Student Ambassador for People to People International that was established by President Dwight D. Eisenhower, as part of the United States Information Agency. She has been to China, Italy, Switzerland, Austria and France.



FEATURED PARTNER



Duo combines security expertise with a user-centered philosophy to provide two-factor authentication, endpoint remediation and secure single sign-on tools for the modern era. It's so simple and effective, you get the freedom to focus on your mission and leave protecting to them.

Feature Partner Product: Multi-Factor Authentication (MFA)

Multi-Factor Authentication from Duo

There's no easier way to use multi-factor authentication. Designed for the modern workforce and backed by a zero trust philosophy, Duo is Cisco's user-friendly, scalable access security platform that keeps your business ahead of ever-changing security threats.

Modern, Effective Multi-Factor Authentication

Multi-factor authentication from Cisco's Duo protects your applications by using a second source of validation, like a phone or token, to verify user identity before granting access. Duo is engineered to provide a simple, streamlined login experience for every user and application, and as a cloud-based solution, it integrates easily with your existing technology.

User-Friendly, Super-Secure Authentication

Adding multi-factor authentication to your security stack doesn't have

to be disruptive to your users. Duo is fast and easy for users to set up, and with several available authentication methods, they can choose the one that best fits their workflow. No headaches, no interruptions — it just works.

Remarkably Scalable MFA Technology

Because Duo functions like a gateway for your existing and future IT infrastructure, it's the perfect solution for growing businesses of any size. Set up new users and support new devices at any time, and protect new applications almost instantly — without impacting legacy technology.

Lightning-Fast MFA Deployment

Finally — a multi-factor authentication solution that isn't a pain in the neck to roll out. Duo can be added to any existing environment or platform, and its self-enrollment feature makes it easy for users to get set up.

Unmatched Coverage

Duo natively integrates to secure any application or platform, so whether you're adding 2FA to meet compliance goals or building a full zero trust framework, Duo is the perfect addition to your security portfolio.

- Multi-cloud, hybrid, or on-premises environments
- SAAS tools, critical infrastructure, custom applications, even SSH
- Secure remote access and VPN clients, BYOD, and even offline devices

Frictionless Authentication Management

With an intuitive administrative dashboard, detailed reporting, and an always-up-to-date cloud-based model, multi-factor authentication couldn't be easier to manage.

duo.com

The Cloud: Connecting us during the COVID-19 outbreak

Governments across nearly every continent issued stay-at-home orders, which apparently slowed the spread of COVID-19. However, while these drastic measures have saved and continue to save countless lives, the negative repercussions to economies, societies, and individuals' mental well-being are enormous. Thankfully, the cloud is playing a substantial role in mitigating the effects on all three.

CLOUD COMPUTING HELPS BUOY ECONOMIES

For many people, being forced to stay at home means being unable to earn money or spend money on in-person services and activities that form dense congregations, such as watching movies or attending concerts. Because of this, the world is projected to enter a global recession, although cloud computing helps to put a damper on this in a number of ways:

- The cloud allows people to work remotely.
- Cloud-based productivity and project management tools let people continue working from the safety of their own homes, thereby helping businesses remain operational despite having empty offices.
- Cloud hosting solutions support eCommerce activities.
- Cloud-based payment systems help keep money flowing.

Communications can be challenging when it's harder for people to talk face to face, but cloud-based apps keep communities together in the following ways:

- Social media apps help disseminate truthful information about the pandemic to the public.
- News agencies disseminate the latest developments regarding the pandemic in real time via social networks such as Twitter. Even government agencies and elected officials like New York State Governor Andrew Cuomo broadcast briefings over social media.
- Chat and video conferencing apps help families and friends keep in touch with each other.
- Much of human communication is actually nonverbal: we discern vocal tone, read body language, and take cues from people's facial expressions. Moreover, as social beings, we crave interpersonal interactions — and seeing each other's faces through video calls and video conferencing is the next best thing.

The cloud is now a ubiquitous part of people's lives, be it personally or in business. To find out the best cloud solutions for your company, [contact our IT experts today](#).

July

" The ultimate promise of technology is to make us master of a world that we command by the push of a button."
- Volker Grassmuck

TIPS OF THE MONTH

Tips to Save You Time!

1. Use your scroll wheel to open a new tab
2. Use the spacebar to scroll up and down a page
3. Search from the browser bar
4. Create templates for frequently used documents

