EasyIT®

REMOTE CYBERSECURITY: BEST PRACTICES FOR MANAGERS & END-USERS

Cybersecurity is a fundamental part of your success in a remote work model. However you secured your remote team at the start of the pandemic, now is the time to take it a step further.

www.EasyIT.com

01

Remote Work Is Beneficial — So Long As It Doesn't Put Your Organization At Risk

The silver lining of remote work during the pandemic is that it has allowed many organizations to realize how beneficial it can be:

- **77%** of remote employees say **they're more productive when working from home**
- **76%** of employees **prefer to avoid their office completely** when they need to concentrate on a project
- **98%** of remote workers want to **continue to work remotely** (at least some of the time) for the rest of their careers

However, for all the ways remote work is beneficial to both the organization and end-users, it's not without its challenges.

You're reading this ebook, which means you're worried about remote cybersecurity to some extent — and you should be. **36% of organizations have dealt with a security incident** due to an unsecured remote worker.

According to **Morphisec's Work-from-Home Employee Cybersecurity Threat Index,** 20% of workers said their IT team had not provided any tips as they shifted to working from home.

02

The Reality Of Remote Cybersecurity

When the COVID-19 crisis hit, it hit fast.

Despite what, in retrospect, may have seemed like a gradual build-up, it was virtually over the course of a single weekend in March that businesses across the US had to pivot to a remote work model.

Obviously, the first priority was maintaining business continuity. You needed to make sure your newly remote workers had the technology and the remote access necessary to do their work.

But the process doesn't end there — security is a complicated undertaking for remote work models, and needs ongoing attention.

Continuing with a remote work model, whether entirely or in part, will require:

- Enhancing security measures
- Providing the right hardware for users working permanently from home
- Implementing more permanent file-sharing and collaboration tools

03

Remote Cybersecurity Considerations For Business Owners & Managers

Even before the pandemic, it was becoming increasingly common for businesses to hire remote workers — that is, staff members that work from home, outside of the business' city of operation, and even much further away.

It's important to recognize that when businesses start prioritizing remote access to data over the security of that data, they make an easy target for hackers.

Think of it this way — at the office, everything is protected by the same set of cybersecurity solutions. You have firewalls, antivirus software, etc. These are defenses that you've invested in and can trust.

Is the same true of your employees' home networks and personal devices? Probably not.

With so many employees operating remotely, working from a laptop or smartphone, how can you be sure that your data is completely secure? Are you taking the necessary steps to maintain security while your staff works from home?

Many owners and managers assume that a VPN is enough to protect their business while managing a remote work environment. That's not necessarily true — one wrong step, and a remote worker can put your network at risk.

04

3 Components Of Organization-Wide Remote Cybersecurity

1

Make Sure You’re Compliant

This may sound obvious, but that's not necessarily the case. Compliance means figuring out which legislation applies to you, what security vulnerabilities you may have been dealing with, and how to integrate compliance into your business processes.

- Determine which data compliance regulations you’re subject to, and which ones may be in the works.
- Do what it takes to become familiar with the particulars of these systems – assign a small team to learn more about compliance.
- Develop a specific risk assessment checklist for compliance.

2

Build A Data Strategy

A well-developed strategy will dictate when, where and how your data is processed, managed and stored. This means laying out how you respond to a data breach, listing who has access to data, tracking where data is stored and accessed, etc.

- Building on the compliance requirements determined in the previous step, develop a strategy that will prioritize management and security for personal data.
- Track the access to and storage of the sensitive data you store.
- Dictate strict back-up and recovery protocols.

3

Make Sure You’re Secure

Security and compliance are inseparable. Both are centered around protecting the integrity of your data. If you’re not secure, then you’re not compliant.

- Audit your IT to identify vulnerabilities that need to be addressed.
- Keep your hardware supported and your software patched.
- Confirm that your data “supply chain” and cloud partners (anyone else who stores or accesses the data for which you’re responsible) are also secure.

Business Owners' & Managers' Remote Cybersecurity Checklist

□ **Two-Factor Authentication:** Two-factor authentication is a great way to add an extra layer of protection to the existing system and account logins. By requiring a second piece of information like a randomly-generated numerical code sent by text message, you're able to make sure that the person using the login credentials is actually who they say they are.

However, this isn't just for websites and common user accounts — 2FA should also be enabled for VPN and Remote Desktops.

□ **Conditional Access:** Conditional Access software gives you the ability to enforce controls on the access to apps in your environment, all based on specific conditions and managed from a central location. It's an extra layer of security that makes sure only the right people, under the right conditions, have access to business data.

□ **Data Loss Prevention (DLP):** A DLP policy tracks sensitive data and where it's stored, determines who has the authorization to access it, and prevents the accidental sharing of sensitive information.

□ **Email Security:** Did you know that 96% of phishing attacks and 49% of malware attacks originate as emails?

That's why you should have a powerful email spam and content filter protecting your organization's inboxes. The right filter will defend against phishing, blatant malware threats, and that don't involve malware, including impostor emails and business email compromise (BEC).

□ **Backups:** Given that many businesses are using cloud-based platforms today, users often assume that their data is automatically backed up to a secure off-site location. But is that really the case?

Reliable backup capability requires additional support. The key is in finding the right third-party backup solution to support your cloud-based accounts. By adding data backup capabilities, you can make sure all your bases are covered.

□ **VPN:** When you use a virtual private network (VPN), your data is encrypted, or hidden, as it moves from your device to the VPN and then continues onto the Internet. That makes it harder for an attacker to identify you as the source of the data.

□ **Endpoint Protection:** EDR is an emerging technology that addresses the need for continuous monitoring and response to advanced threats.

This is a vital service that protects endpoints like laptops, desktops, smartphones, tablets, servers, and virtual environments. Endpoint protection may also include antivirus and antimalware, web filtering, and more.

06

What About Your End Users?

Did you know that more than 90% of cybersecurity incidents can be traced back to human error?

Cybersecurity awareness training is an essential part of an effective remote cybersecurity defense. Are your staff members supporting your cybersecurity? Or putting it at risk?

The fact is that what you (and your staff) don't know could hurt you. If your staff isn't up to date on the latest cybercrime scams, then they're putting your data at risk, simple as that.

The key to truly comprehensive cybersecurity is simple, yet often overlooked: the user.

The best cybersecurity technology and practices in the world can be undone by one staff member who doesn't understand how to use them, or how to protect the data they work with.

The right training services will offer exercises, interactive programs, and even simulated phishing attacks to test your staff on a number of key areas:

- How to identify and address suspicious emails, phishing attempts, social engineering tactics, and more.
- How to use business technology without exposing data and other assets to external threats by accident.
- How to respond when you suspect that an attack is occurring or has occurred.

Are Your Employees Defending Against Phishing?

CISA has issued a warning to US businesses about the increase in phishing and other social engineering scams over the course of the pandemic. CNN even reported a 500% increase in phishing attacks when the pandemic began.

Do you and your staff members know how to spot a phishing email? You better make sure — the **average phishing attack costs businesses $1.6 million.**

Phishing is a method in which cybercriminals send fraudulent emails that appear to be from reputable sources in order to get recipients to reveal sensitive information and execute significant financial transfers.

Phishing attacks are mass emails that request confidential information or credentials under pretenses, link to malicious websites, or include malware as an attachment.

With only a surprisingly small amount of information, cybercriminals can convincingly pose as business members and superiors in order to persuade employees to give them money, data, or crucial information.

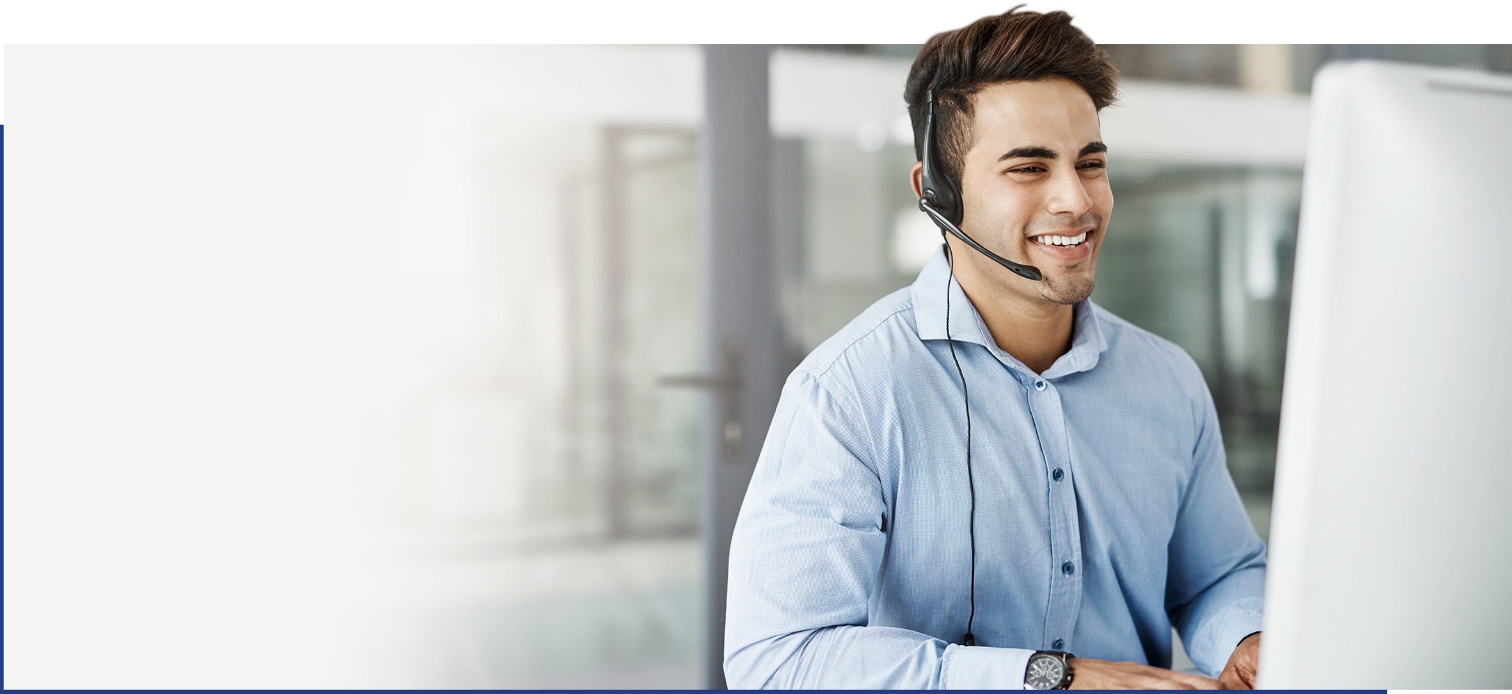
08

Make Sure Your Staff Knows How To Maintain Remote Cybersecurity

There are 14.5 billion phishing emails sent every day — you need to know how to spot them:

- **Check The Right Fields:** If you're unsure about an email, check the details on the email itself – specifically the "mailed-by" and "signed-by", both of which should match the domain of the sender's address.
- **Suspicious Links:** Always be sure to hover your mouse over a link in an email before clicking it. That allows you to see where it actually leads. While it may look harmless, the actual URL may show otherwise, so always look, and rarely click.
- **Spelling and Grammar:** Modern cybersecurity awareness comes down to paying attention to the details. When reading a suspicious email, keep an eye out for any typos or glaring errors. Whereas legitimate messages from your bank or vendors would be properly edited, phishing emails are notorious for basic spelling and grammatical mistakes.
- **Specificity:** Another point to consider is how vague the email is. Whereas legitimate senders will likely have your information already (such as your first name) and will use it in the salutation, scammers will often employ vaguer terminology, such as "Valued Customer" - this allows them to use the same email for multiple targets in a mass attack.
- **Urgent and Threatening:** If the subject line makes it sound like an emergency — "Your account has been suspended", or "You're being hacked" — that's another red flag. It's in the scammer's interest to make you panic and move quickly, which might lead to you over looking other indicators that it's a phishing email.
- **Attachments:** Phishers will often try to get you to open an attachment, so, if you see an attachment in combination with any of the above indicators, it's only more proof that the email is likely part of a phishing attempt.

In the end, the key to phishing methodology is that it doesn't rely on digital security vulnerabilities or cutting edge hacking technology; phishing targets the user, who, without the right training, will always be a security risk, regardless of the IT measures set in place.



Need Expert Guidance In Managing A Secure Remote Workforce?

If you plan to continue with remote work in one way or another, you may need to change your model of IT support — as you and the other c-level executives at your business have likely discovered since the start of the pandemic, your ability to work remotely and securely depends directly on your IT support.

In the remote setting, technology is necessary so that you and your staff can:

- Access files, applications, and systems from a remote setting
- Collaborate with colleagues, partners, and customers via video conferencing solutions
- Stay secure against the increased rate of phishing attacks related to the pandemic
- Maintain communications with cloud-based phone systems that keep staff connected

EasyIT can help — over the course of the pandemic, we've gained extensive experience in helping our partners to launch, optimize, and secure remote work capabilities.

Now that the mad rush to go remote is over, it's time to perfect your processes. You don't have to do so alone.

Get in touch with the EasyIT team to get started.

www.EasyIT.com • (614) 339-4999
sales@EasyIT.com

EasyIT®

www.EasyIT.com | (614) 339-4999 | sales@EasyIT.com
4150 Tuller Road, Suite 212 • Dublin, OH 43017