

# 7 Urgent Security Protections Every Business Should Have In Place Now

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are “low hanging fruit.”

***Don't be their next victim!***



**NetCare**  
PROTECTION PLUS  
provided by Link Computer Corporation

# Are You A Sitting Duck?



**Small and medium businesses, are under attack.** Right now, extremely dangerous and well-funded cybercrime rings in China and Russia are using sophisticated software systems to hack into thousands of businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses.

**Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot?** Think again. 560,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

In fact, the National Cyber Security Alliance reports that one in five small businesses have been a victim of cybercrime in the last year – and that number is growing rapidly as more businesses utilize cloud computing, mobile devices and store more information online. You can't turn on the TV or read a news article without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity.

## Because Of All Of This, It's Critical That You Have These **7 Security Measures In Place.**

1

### **Train Employees On Security Best Practices**



The #1 vulnerability for business networks is the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

**To Request Your FREE Cybersecurity Risk Assessment,** please visit [www.linkcorp.com](http://www.linkcorp.com) or call our office at 814-742-7700.

## 2

### Create An Acceptable Use Policy (AUP) – And Enforce It!



An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the web sites employees can access with work devices and Internet connectivity. Further, you must enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what web sites your employees' access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

Having this type of policy is particularly important if your employees are using their own personal devices to access company e-mail and data.

If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, it can be a gateway for a hacker to enter YOUR network. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of the employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured; but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

## 3

### Require Strong Passwords And Passcodes

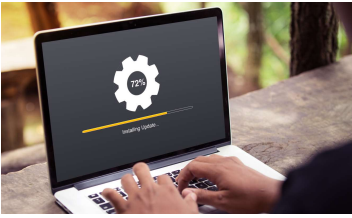


Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. This can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

To Request Your **FREE** Cybersecurity Risk Assessment, please visit [www.linkcorp.com](http://www.linkcorp.com) or call our office at 814-742-7700.

4

## Keep Your Network Up-To-Date



New vulnerabilities are frequently found in common software programs you are using, such as Microsoft 365; therefore, it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated, so you don't have to worry about missing an important update.

5

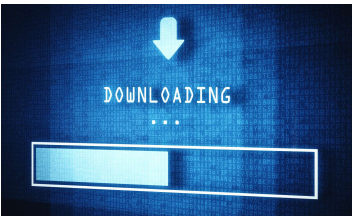
## Have An Excellent Backup



This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it to work!

6

## Implement a Managed Endpoint Detection & Response solution



MDR detects unknown threats as well as known viruses. In addition it will automatically contain these threats to protect your environment and alert the Security Operation Center (SOC). The SOC agents will proactively investigate and remediate the threats.

7

## Don't Scrimp On A Good Firewall



A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT person or company as part of their regular, routine maintenance.

To Request Your **FREE** Cybersecurity Risk Assessment, please visit [www.website.com](http://www.website.com) or call our office at XXX-XXX-XXXX.

# Want Help Implementing These 7 Essentials?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

At no cost or obligation, we'll send one of our specialists to your office to conduct a free **Cybersecurity Risk Assessment** of your company's overall cybersecurity posture. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll have these questions answered:



Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?



Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).



Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?



Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines.



Is your firewall and antivirus configured properly and up-to-date?



Are your employees storing confidential and important information on unprotected cloud apps, like Dropbox, that are OUTSIDE of your backup?

To Request Your **FREE** Cybersecurity Risk Assessment, please visit [www.linkcorp.com](http://www.linkcorp.com) or call our office at 814-742-7700.

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the businesses we've audited over the years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a third party to verify nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

## You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Cybersecurity Risk Assessment**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.



Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

**You've spent a lifetime working hard to get where you are.** You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at **814-742-7700** or you can e-mail me personally at [mstrait@linkcorp.com](mailto:mstrait@linkcorp.com).

Dedicated to serving you,

Mike Strait

Web: [www.linkcorp.com](http://www.linkcorp.com)

E-mail: [mstrait@linkcorp.com](mailto:mstrait@linkcorp.com)

Phone: 814-742-7700

**To Request Your FREE Cybersecurity Risk Assessment,**  
please visit [www.linkcorp.com](http://www.linkcorp.com) or call our office at 814-742-7700.

# Here's What A Few Of Our Clients Have Said:

## Link Computer is like having your own IT department at your fingertips 24/7!

Having the entire Link team with an eye on our system's security and health has lifted a huge weight off my shoulders. They answer any questions I have and create recommendations based on our environment.

We have not worked with IT firms in the past but through the vetting process, Link truly made it feel like we were entering into a partnership. They made sure everything we wanted was covered and also had further recommendations to have a more secure environment.

The employees at Link are extremely knowledgeable in their field and do not hesitate to take the time to explain any questions you have thoroughly. We have had a lot of encounters with software help desks where you never talk to the same person twice and your questions never seem to be answered or changes never appear to be completed. A huge plus for us was each time you call/e-mail the Link help desk you know who you are talking to, and they are prompt.

– Danielle Siebert, Operations Manager, Armstrong County Building & Loan Association

## We chose Link because of their proven track record

We chose Link because of their proven track record. They were brought in to secure the borough's network. Link delivered top level communication, while the other providers constantly left us waiting.

Link has been an easy switch for us. Cost are down, our network is up and backups are completing. We have the support we can count on and trust. Link has made the management of the borough's systems and network completely worry-free.

– Gary Kuklo, Mount Union Borough

## Link's commitment to quality customer service has been key...

The greatest advantage of partnering with Link Computer is the immediate access to IT support for all the staff.

Link's commitment to quality customer service has been key to improving our employees' morale and performance. Communication has been excellent at all levels in the company.

Link truly listens to you! They gather information about your issues, your budget, as well as your dreams and develop a business plan that is feasible, dependable, and affordable. They are professional in every aspect.

– Connie Brode, Executive Director, Huntingdon Bedford Fulton Area Agency on Aging

To Request Your **FREE** Cybersecurity Risk Assessment, please visit [www.linkcorp.com](http://www.linkcorp.com) or call our office at 814-742-7700.

# To Request Your FREE Cybersecurity Risk Assessment:

1. Go online to [www.linkcorp.com](http://www.linkcorp.com)
2. Call us direct at **814-742-7700**.
3. E-mail your appointment request to **Mike Strait** at [mstrait@linkcorp.com](mailto:mstrait@linkcorp.com)



**NetCare**  
PROTECTION PLUS