The IT Insider

November 2018

PREVENT CYBER CRIME: WHAT NOT TO DO

Cybersecurity is arguably the most important aspect of any business plan. Businesses, especially small businesses simply cannot survive a major data disaster.

Here are 4 Don'ts to help you prevent cybercrime.

These four "don'ts" below will help you and your staff to keep cybercriminals out of your network and out of your pockets.

Preventing cybercrime is becoming more and more important as technology improves and the cybercriminal industry grows. Cybersecurity is arguably the most important aspect of any business plan. Businesses, especially small businesses simply cannot survive a major data disaster.

Improving your company's cybersecurity is not one big effort - but several small ones. These four "don'ts" below will help you and your staff to keep cybercriminals out of your network and out of your pockets.

Don't use the same password for everything.

Ideally, every single username/password combo will be as different as you can make them. Of course, you should never use the same password as a coworker. You should also never use your coworker's login information to log in a computer. This sharing of sensitive information makes your network weak.

It's also vital to craft passwords that are up to industry standards. Choosing a strong password is your first line of defense when it comes to unauthorized access to your computer or network. Using passwords that are easy to guess (many cybercriminals actually have computers that use algorithms to guess your passwords) is setting yourself up for an attack. Use a password manager for ones that you can't memorize - don't leave the password written on a sticky note at your desk.

Don't ignore updates or patches.

We get it - updating Java or your anti-virus software can get annoying and frustrating. It happens so often! However, whether it's an update to your cell phone, your operating system, or a software application you should always keep them up to date.

These updates and patches have very important jobs to do. A large chunk of these updates are centered on

Improving your company's cybersecurity is not one big effort - but several small ones.

cybersecurity - the newer versions will block newer viruses and malware. They seal up holes in the applications or software that were used to gain illegal access. Every day, cybercriminals find new ways to access networks and gain control of data - updates and patches help keep those criminals out.

Don't let strangers use your network or hardware.

You probably wouldn't hand your credit card to a stranger - so don't do it with your WiFi network or your laptop. It may come across as rude, but firmly deny access to anything electronic you own that could provide a stranger with information about you. Your phone, your computer, your WiFi password, etc.

Make sure you trust the person using your laptop as much as you'd trust them with your credit card. It's essentially the same thing - having access to your network or hardware is giving a stranger access to some very intimate details about your life. If you've ever shopped or banked online, they can get your bank information. They can access your email address. If you're on a shared network at your office, they may be able to find the W-2s of every employee or the sensitive client information stored there.

Don't try to prevent cybercrime on your own.

Preventing cybercrime is not easy, so it's best to let an IT support team handle it. This is a big job, so let the professionals help you out. You're an expert at your job, and we're an expert at ours. Our job is to protect our clients from cybercrime. We can provide you with the training and tools you need to keep cyber attacks from happening to you and your company. Plus, in the event a cyber attack does happen, we can help you recover from it.

Does Your Business Have a Disaster Recovery Plan?

What is your strategy for the aftermath of a terrible storm or aggressive ransomware attack? Likely, you have insurance on your building and your physical belongings like desks and computers and the coffee maker. But what about your data? What about the information stored on your server? Believe it or not, while the server itself may be covered by your insurance policy, everything it contains within its drives is not. For that, you need cyber insurance, which we do recommend, but even that won't help you recover lost data that you need to run your business. While a cyber insurance policy may provide a much-needed payout, it won't magically bring back all of those vital files, information, and software you need to run to your business every day.

We briefly discussed a disaster recovery plan in our blog about business continuity. Both are essential parts of business planning, but disaster recovery is the meat and potatoes of your Business Continuity Plan.

Life is unpredictable. Business is, too. The more you can control about the future of your business, the better off you'll be in the long run. This is where disaster recovery comes in. Disaster could occur at any time. Whether it's a fire, a break-in, a storm, or even a disgruntled employee. By putting forth a plan for disaster and the recovery process after the fact, you will be far better off. In fact, disaster recovery is becoming required by more and more business insurance policies. With technology growing so steadily, you should expect your insurance company to demand a written disaster recovery plan sooner rather than later.

Here's what you need to include:

A general prevention audit. What are the key assets that need protecting? List the ways in which these assets are protected and audited regularly for safety.

Your recovery team. In this section, you should outline the management team roles during and after a disaster. Make sure these people are trained to know their roles and tasks during a disaster. They will need to know when and how to implement the recovery plan.

Emergency response. List an overview of what you consider a disaster, and which recovery plan your team should execute.

Communication plan. It's best to establish a kind of phone tree for disasters. Nominate a person (and a backup person) in each area of your business who is in charge of reaching out to a specific set of employees.

Recovery strategies. Finally, you should include a section on recovery. What needs to be implemented in order for your business to recover from a large fire? Where, if necessary, is your alternate workplace?

It's important to update this document as often as you can. Anytime you change assets, hire new management, expand your building, etc. make sure you revise your disaster recovery plan.

This device can spin up your business (your files, your data, your software, anything, and everything) in the cloud so that you can function as close to normal as possible during a disaster. Your employees will be able to work out of this digital space until your physical one is ready again. Your clients shouldn't even notice a difference.

PREFERRED IT SECURITY SPOTLIGHT

We all make mistakes, but sometimes those mistakes can have drastic consequences. Make sure that you are following these quick and easy tips to stay safe both in your office and online.

1. Leaving machine on and unattended.
Make sure you lock your computer when you walk away from it. This ensures that whatever you're working on is safe from passers-by.

2. Opening email attachments.
Do not blindly open email attachments. If you aren't expecting the attachment, don't open it. Watch out for invoices and resumes, which are the two most popular hacker tricks. Read more about ransomware here.

3. Using a poor password.
Most passwords can be easily guessed by a hacker within 10 minutes. Make it harder for them by adding special characters like an exclaimation mark or a hashtag.

4. Connecting to unsecured wifi.
When connecting to wifi, make sure you are someplace safe like your home or office. Try not to connect to "free wifi" like those found at Target or McDonalds.

5. Not backing up your data.
Make sure you have a backup device or solution. Are you backing up your data on site or in the cloud? How often are you backing up?

6. Trusting too much.
Social engineering is on the rise, and hackers are using it to infect your system with viruses. Don't give out personal information over the phone or online.

Want To Know For Sure If Your Data Is Safe?

Thanks to our Done-For-You Disaster Recovery you can rest assured that your data is being backed up in a format that is not only secure, but also easily recovered when you need it.

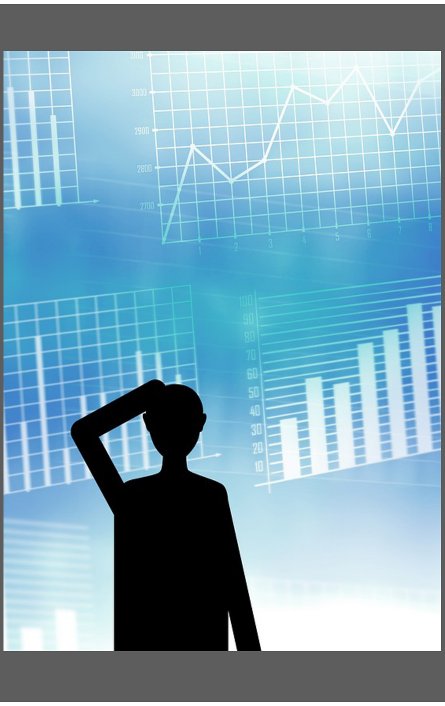
Your files are automatically backed up every hour locally and over the Internet.

Your data is safe from fire, floods, storms, viruses, hackers, hardware malfunctions, and human error! With image-based and file level backups, your data is immediately accessible even during a disaster.

Should a disaster occur, you can be back up and running the very same day…we **GUARANTEE** it.

Preferred IT Group will provide the hardware required, **absolutely free**.

Learn more at www.preferreditgroup.com/dfydr



OUR COMMUNITY

Help out a neighbor, and get put in our giveaway contest!

If you know of a business owner who have 10 or more employees in northeast Indiana in need of IT services, let us know!

Anyone you refer will receive a free Network Health Check (a $1,675 value), plus you'll get an Amazon gift card.

We'll also enter you to win our quarterly referral contest - this quarter the prize is an Rtic Cooler (filled with your favorite beverage)!

preferred IT group

CONTACT US

Fort Wayne	Warsaw
260.440.7377	**574.306.4288**
Columbia City	Indianapolis
260.213.4266	**317.426.8180**

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.