February 2019
http://www.ctsioutsourcing.com
229-446-9641

NEWSLETTER

Phishing attacks have been around for a long time in IT. Designed to steal your credentials or trick you into installing malicious software, they have persisted in the IT world precisely because they have been so devastatingly simple and effective. Today, a more modern and more effective version of the same attack is commonly used.

A typical phishing attack involves an attacker sending out a malicious email to hundreds of thousands, if not millions of users. The attacker's email is designed to look like it comes from a bank, financial service, or even the tax office. Often aiming to trick you into logging in to a fake online service, a phishing attack captures the login details you enter so an attacker may use them to enter the genuine service later.

By sending out tens of thousands of emails at a time, attackers can guarantee that even if only one half of one percent of people fall for it, there is a lot of profit to be made by draining accounts. Spear phishing is a more modern, more sophisticated, and far more dangerous form of the attack. It's typically targeted at businesses and their staff.

A Convincing, Dangerous Attack

While a traditional phishing attack throws out a broad net in the hope of capturing as many credentials as possible, spear phishing is targeted and precise. The attack is aimed towards convincing a single business, department, or individual that a fraudulent email or website is genuine.

The attacker focuses on building a relationship and establishing trust with the target. By building trust and convincing the target that they are who they are pretending to be, the user is more likely to open attachments, follow links, or provide sensitive details.

Consider how many times you have followed a link or opened an attachment just because it has come from a contact you have trusted before.

A Trusted E-mail

The malicious email can appear to come from a vendor you deal with regularly. It may even look like an invoice you are expecting to receive. Often attackers can simply substitute the vendors' banking details for their own, hoping the target will not notice the difference.

Such an attack is very difficult to detect. It takes a keen eye, strong working knowledge, and constant awareness to keep your company protected. Even a single small mistake by an unaware member of staff can compromise your business accounts.

Defending Your Business

The key to stopping a spear phishing attack is education. Learning attack techniques, and how to protect against them is the single biggest thing you can do to enhance business security.

Whenever you deal with a vendor in a business transaction, you should always consider important questions before proceeding. Are you expecting this email? Is the vendor attempting to rush you into a quick decision or transaction? Have you checked all the details are correct and as you expected? Sometimes a simple query to the vendor can protect you against worst-case scenarios.

In many cases, a phishing attack can be halted in its tracks with a strong IT security package. Web filtering prevents malicious emails and links from entering the network, shutting attacks down before any damage can be done.

Good Security Practice

As with many types of IT threat, good security practices help mitigate damage. Locking down security to ensure employees only access the systems they need helps to prevent damage spreading across the network.

Enforcing unique and strong passwords prevents leaked credentials from affecting systems related to the one that has been compromised. Getting employees set up with a password manager and good security policies can do the world of good to boost your security to the level it needs to be.

Give us a call at 229-446-9641 to audit your security practices. It could be the difference that secures your firm against sophisticated spear phishing attacks.

"Upward growth often requires new office technology"

Professional Businesses Deserve Professional Setup

Watching a business grow is as satisfying as it is rewarding. Whether opening a new office, starting a new department, or bringing in a new employee; it's a positive step in the right direction. Upward growth often requires new office tech and IT changes to bring new staff fully online.

At a minimum, a new computer will be needed for employees to get started quickly and hit the ground running. New staff or an entire department may require a server, printer, or additional networking hardware to cope with extra demand.

A tech smart business should give careful consideration to how it sources and sets up its hardware and software. It can be tempting to pick a simple solution off the shelf from the nearest retailer.

Modern manufacturers often make it easy to get set up with a new device straight out the box. Using default settings and a simple setup means a laptop or tablet can be just plugged in and it's ready to go, right?

Unfortunately, setting up technology to create safe, secure, and reliable business services requires a little more detail.

Setting Up Tech For Business

The hardware you have is at least as important as the hardware you buy. It's important to ensure new tech on the network is compatible with your existing business systems. Adding the wrong solutions to accommodate new employees can slow down the system for everyone.

Many firms talk themselves into buying the most expensive, or heavily marketed system on the market. Buyers often feel confident that the high price tag and slick design means it's guaranteed to work with anything you put to it. We wish that were always the case.

Without an eye for fine detail and good IT knowledge, combining certain solutions can cause a significant network slowdown or even fail to work together at all.

Consistency Is Key

It can seem easy, and tempting, to buy technology based on offers and deals around at the time you need it. Some companies do this to save money short term, building their systems using a mixture of hardware from various vendors and manufacturers. When thinking long term, this approach might not get you the great deal that you think.

Mixing suppliers alone can make it difficult to track where components came from in the coming months and years. Warranties, service agreements, and support can become hard to track down when parts fail and hardware dies. Money spent securing your business against failure is completely wasted if you can't find the right paperwork at the right time.

Sourcing replacement parts and supported peripherals can be made more difficult when components are mixed too.

Planning ahead and purchasing identical hardware can make swapping components fast and straightforward. When systems are consistent, both parts and knowledge can be shared throughout the entire business. A smart decision today can eliminate costs, time, and headaches further down the road.

Unexpected issues appearing at the last minute can have large consequences on workload and deadlines. Sharing everything from chargers to memory can help to reduce and mitigate IT risks. Consistent hardware, swappable components, and even considering a supply of spares can take care of many potential headaches.

Smooth Onboarding

In business, first impressions are critically important. Whether setting up a new office or getting an employee ready to start, a professional attitude goes a long way. Good IT that's ready to work sets a professional tone to carry your business forward.

IT that supports and enhances operations is infinitely better than IT that gets in the way. Using consistent and well-known solutions in the right way avoids wasting time, maintains performance, and reduces costs where it matters.

Our goal is to ensure your hardware meets your business needs. A professional setup ensures your IT is consistently improved while you watch your business flourish and grow.

Give us a call at 229-446-9641 for a professional setup to make sure nothing stands in the way of growing your business.

Is Your Physical Security as Good As Your Cybersecurity?

"How would your business be protected if the attack came from within your firm?"

Headlines are often made by firms that have been hacked by "elite" cybercriminals. These events sound high tech, sophisticated, and interesting. The truth is almost always an amateur attacker chancing their luck with an unpatched security hole or bad password. Physical break-ins affect businesses far more commonly and cause much more damage, but get talked about far less.

Similar to technology hacks, most physical security threats come from criminals that chance their luck on businesses that look poorly secured. On a rare occasion, they may strike a business owner that has forgot to lock up or failed to set the security alarm.

By breaking in, these criminals exploit poor physical security to cause damage and steal valuables. Typically, by destroying or taking critical assets, a criminal may make a few hundred in profit while the total damage done to the business is counted in the tens of thousands.

While most IT security packages act automatically and always remain on, physical security needs to be made a daily habit and require periodic updates.

Threats Starting from Within

Every business should have secure locks protecting their doors. Many use an alarm system to add protection to valuable assets. However, there are common threats that neither of these can protect you from. How would your business be protected if the attack came from within your firm?

A disgruntled employee, or even a former employee, can do an enormous amount of damage to a business. Attacking their own business, an employee can likely do more damage during the day than a criminal could breaking-in overnight. Misplaced trust in the wrong individual can result in devastating consequences.

Employees typically have access to one of your business's most valuable assets: data. A criminal may steal computer hardware to sell on for quick cash because most don't fully understand the value of the data stored on it.

The value of the data in a business machine can easily exceed the cost of the hardware one hundred times over.

Physical Security Heists

For criminals who do understand the value of data; physical security can be the weakest spot in a business's armor. In 2013, media streaming service Vudu suffered a break in where criminals stole server hardware to obtain credit card information stored within.

A technology savvy streaming firm is highly likely to have up-to-date IT with excellent security measures. Thieves looking for easy cash recognized that the best way to get to the data was through their comparatively weak physical security.

The best security packages in the world are completely infective if the keys are left in the door and physical hardware is easy to remove. This challenge of securing your data can be made even more difficult when using a location that must remain open to the public.

Securing Your Data with Good Security Practices

Keeping your customer data safe is one of the most significant responsibilities small business owners take on. It requires a duty to employ the best possible security practices to keep your customers safe. For a customer to have the trust to use your business over the competition, they have to see their concerns put to rest.

Locking down data access for employees so they can only view and edit what is strictly needed, protects both customers and the business against many kinds of damage; both accidental and malicious. Limiting device access, such as disabling USB ports to thumb drives or storage devices, helps to prevent data being copied and carried offsite.

Physically locking down a server in the location it sits is one of the best deterrents available to prevent against theft. Locked server racks are an excellent piece of physical security that works on top of the building security already in place.

Make sure your business is up to the task of securing its data. Give us a call at 229-446-9641 to audit both your digital and physical security.

Invest Well in Your IT Security

If it ain't broke, don't fix it' is a common and useful rule for many business owners. It serves to protect your business against unnecessary costs and unneeded downtime. While protecting your business against many types of danger, it poses an outright threat when it comes to IT security.

Security threats to your firm move so fast that your IT should be working twice as hard as your company just to keep up. Every day, hundreds of thousands of new malware threats are released. Falling even hours behind means any one of these attacks can threaten your business.

The single most dangerous thing IT security can do is stand still. Keeping up with the latest advice, technology, and updates the security industry offers is vital to keep your business safe. This makes up much of the unseen job of IT professionals. Hackers never stop looking for new ways into your system, which means your security can't stop looking for ways to keep them out.

Modern Systems for Modern Business

One of the most common security threats a business opens itself to is using an outdated operating system or software package. Many firms are scared to upgrade, update, or renew their IT over fears of breaking legacy systems. Many rely heavily on old software and are afraid to make a large change themselves. Some businesses today still run machines on Windows XP, an operating system first released back in 2001.

Old operating systems stop receiving security updates and patches that protect against newly released attacks. These systems become very vulnerable, presenting a large target for knowledgeable hackers. This happens many years after newer versions have been released, giving knowing IT firms a chance to migrate safely.

Hackers are always on the lookout for businesses that run IT equipment outside of its suggested service life. A server, desktop computer, or peripheral is a golden opportunity for criminals to enter and threaten a business.

Hackers purchase their attacks on the dark web, safe in the knowledge that old systems won't be patched. These attacks can then be used to attack unguarded firms to steal or compromise vital company data.

An unpatched old machine is like a valuable security door left propped open overnight, a golden opportunity for thieves.

Smart Budgets

Budgeting for business is a difficult task. We aim to make the most of everything we spend and reduce spending as much as we can. IT security can easily fall very far down the list of priorities.

IT can seem like an easy way to cut costs. It's a department that the customer doesn't always benefit from directly, and when it's working well, it might not be on the radar at all. Despite working largely behind the scenes, successful IT is one of the critical components of every highly successful firm. Good IT can be the binding glue that holds the company together.

Even businesses far removed from the IT world typically uses payment machines, ordering systems, and inventory. Even restaurants and retail stores rely on computers to operate. Downtime for any critical system can be a complete disaster. A business can be unable to trade, and costs can mount up fast.

When vital IT components are used by the customer, a sales website, or an automated booking system for example, the problem can multiply tenfold.

Keep On Top Of The Essentials

Good IT isn't built on high peaks and deep troughs in the yearly budget. The kind of IT that makes your business and helps it to grow is built by smart financing and careful planning. Great technicians are what makes excellent IT.

Maintaining steady updates, keeping pace with the latest security, and building your IT as you build your business keeps you in the driving seat when it matters most.

Comnet Technical Solutions, Inc.
CTSI
CTSIoutsourcing.com
229-446-9641

1200 Whispering Pines Rd
Albany, GA 31707

Monday to Friday
8:30am - 5:00pm

CTSI Facebook

When IT is planned and issues are solved before they appear, security becomes cheaper, easier, and many times more effective. System upgrades can be planned out months, if not years in advance so you are never caught unaware.

Don't let your IT be broken before you take steps to fix it. Move ahead of the curve and give us a call at 229-446-9641 so you don't have to find out what your business looks like without IT.