bigfish TECHNOLOGY

Keeping You in The Loop

Password Manager

You haven't updated your password for: *365 Days.*
We recommend you to update your password at least once a year.
Do you want to update your password now?

[YES] [NO]

Time to Refresh Your Passwords

We often tend to be creatures of habit, particularly when it comes to technology. Passwords are a prime example. Many of us use the same logins for multiple websites and applications because we don't have a photographic memory. A large percentage of users aren't aware that this is one of the most significant security dangers they can face online. It has a simple fix too.

Regularly, in the news today, there are stories about major companies being hacked, their customer data stolen, and their customers left stranded. Hackers commonly use data stolen from one site to access others where login credentials have been reused between accounts. In some cases, access to bank accounts has been gained simply by using a compromised email account.

Businesses and individuals can face significant losses simply because a third party outside their control has been hacked or compromised.

The Danger of Old Passwords

MySpace is a key example of why old and possibly forgotten services pose a security danger when passwords haven't been regularly changed. Once a thriving popular network, the use of MySpace services declined drastically from 2007 onwards. While many people moved to new social networks, old accounts typically remained abandoned on their servers. Hundreds of millions of accounts remained on MySpace servers many years past the firm's peak.

In 2016, MySpace suffered a data leak which exposed usernames, emails, and passwords of 360 million user accounts. Shortly after the hack, these details were published online for anyone to see. Many were used to access email accounts, servers, and accounts that shared the same details.

Shared Responsibility

Even if you have never had a MySpace or social media account personally, how many of your employees or coworkers have one or more? Many have had more social media, forum, or game accounts than they care to remember. Have their passwords been updated since 2016?

Your business network protects your systems, work, and intellectual property. For many firms it's the single most critical component, the backbone to business operations. Keeping it secure regardless of the number of people, staff or clients using it is a crucial task.

Consider how many people currently have access and how many of those may reuse their password on another website or service. Just reusing your password once can expose you to the hacking of a third party entirely out of your control.

Password Management

Good security practice is to use a unique and strong password for every login you use. A strong password should include, where possible, capital letters, lowercase letters, numbers, and character symbols. Many consider this

impractical or even impossible, but it is entirely achievable for every firm.

It is clearly impossible to manually remember a strong password for each one of the dozens of logins needed today. Few would even attempt to. A password manager makes storing, retrieving, and using unique passwords easy.

When using a password manager, an individual is required to remember only one single strong password to access a database which contains a different login password for each service. This database can be synced between multiple devices, saved and backed up to the cloud, and even used to create strong passwords for you.

Strong Protection

Password managers can be used to implement security policies that demand zero password reuse, between services or over time, and set strict limits over the duration a password can last. With the right policies in place, both your business and your employees are protected against attacks from hackers that have compromised third-party sites.

The maximum recommended lifetime of a password for any service is a single year. Make the start of the calendar year the time which you refresh your passwords and start new.

To help keep on top of your security and make sure your firm is safe well into the new year, give us a call for more information at 281 318-1680.

Preparing Your Business Tech to Start the New Year

The start of a new year is a challenging time for businesses. It can be a good time to reflect on the wins and losses of the previous twelve months. It's also an excellent time to take stock and evaluate what your business needs to go forward.

IT demands move at a staggering speed, meaning last year's tech may not fit next year's needs.

The new year can bring major change to both the business and the environment it operates in. Regulations, contract terms, and seasonal spending habits mean that adaptations have to be made for continued growth.

A smart business knows how and where to incorporate flexibility to win more business and adapt to a new environment. As we move into the new year, there are fundamental questions we should ask about our IT to ensure we are ready to tackle the next twelve months too.

Is Your Hardware Still Up to The Task?

Businesses are often challenged by their client's demand for files that seem to continually increase in size and resolution. The storage needed to handle, use, and archive these enormous files appears to grow at a near exponential rate.

Every device today is capable of capturing more data at a higher resolution than ever before. Huge data needs have become the new standard.

The expectation of bigger and bigger data is only set to continue as we progress into another new year. Many clients expect, or demand, exceptional quality from professional services and with a fast turnaround time too.

These competing demands put as much strain on network hardware and computing power as they do physical storage. One of the most important things a business can do when reviewing IT demands is to ensure there are no bottlenecks in the productivity pipeline.

Is Your Backup Reliable and Ready?

Almost every business in the modern day has learned enough to put a backup in place. Whether simply transferring files manually to USB storage, copying documents over to a local server, or saving media to the cloud. However, not every business is testing their backups. Fewer still are testing them reliably.

A backup is only as good as what we know can be reliably restored from it. Cases have emerged where big-name firms had famously believed they were backing up successfully for months or years, only to find out their backup was failing when they really needed it.

Whether impacted by missing assets, unable to transfer files, or affected by corrupt data, an untested backup may be as useful as not having any backup at all.

A critical goal for the safety and reliability of any business should be to have dependable backups that are tested at regular intervals.

Is Your Compliance Still Up to Date?

Nearly every business in the world has compliance and regulations standards it must adhere to if it is to keep its position in the marketplace. These may be industry specific such as medical or automotive certifications, or regional protections such as data protection regulations.

Requirements for each of these areas change regularly. It is up to each firm to keep on top of both changes to rules and changes to the firm which may impact them.

Changing IT can often impact certifications in a big way. Many feature rules which affect storage, processing, or altering the way in which data is used; it's essential to check your usage against strict requirements relevant to your business.

While time-consuming and difficult, these checks require a strong knowledge of both the rules and your IT system.

The penalties for failure can be severe and crippling. It is a critical area of the firm you can't afford to get wrong.

If you are looking to boost your business in the new year, check up on your systems and technology, or dust up your certifications to the latest standard: there's never a better time than now.

Give Big Fish Technology a call at 281 318-1680 to get your new year off to a flying start.

What Hackers Target in Small Businesses

"The best defense against ransomware attacks is an up-to-date offsite backup"

Hackers today have many ways to attack small businesses and business owners. Many attempt to use technology to send malware, viruses, or phishing attacks; or use information to con owners and employees into handing over more information than they should.

One or more of these techniques can be combined with gaining physical access to steal from vulnerable firms. Identifying precisely how criminals target businesses and what they deem most valuable can help to protect from the most devastating attacks out there.

Remaining vigilant and informed is one of the most vital things you can do as a business owner to protect your assets and reputation.

Extortion

Different types of attacks tend to rise and fall in popularity. Fifteen years ago, computer worms were the most common attack that businesses faced. Security software wasn't as advanced or as widely used at it is today. Computer worms were, at the time, an exceptionally low-cost and efficient way to inflict the maximum amount of damage for minimum cost.

Today ransomware has seen an unfortunate boom in popularity. This technology aims to encrypt the target's files on their personal computer. This technique denies the victim access and charges a large fee in exchange for the key to retrieve the victim's own data.

The attack has worked so often because it requires minimal effort and can be used again and again. Many businesses have no option but to pay because the data is worth far more than the ransom demand the hackers have made.

The best defense against ransomware attacks, in addition to strong online security, is an up-to-date offsite backup — one that is tested to work reliably.

Targeting Customer Records

One of the most important things for your firm to take care of is your customer data records. Records which include names, dates of birth, and other personally identifying details. These details are extremely valuable to hackers or criminals who, either use them personally or sell them on to someone who will.

Many regions have strict laws and guidelines about how this information must be stored, accessed and protected. Failing to follow these can result in severe penalties that could devastate any company.

Targeting Financial Information

Like personal information, a small business must take extreme care when storing customer financial information. Sensitive details such as credit card or banking information are a key target for hackers looking to steal money fast.

The impact on your business reputation following a breach of financial data will be severe and devastating. Even a simple mistake can require years of advertising and great PR to repair. Many firms have failed to recover after losing the trust of their customers.

Social Engineering

Most firms today run good IT security packages to protect against online attacks and other forms of malware. Attackers often know to take their methods offline to achieve the best results.

Whether posing as a supplier, customer, or interested party; attackers can seek to gain information that you may be less than willing to hand over to a stranger. Small businesses can often be used to gather information on vendors and suppliers they do business with in order to attack them too.

Be particularly cautious of the information you provide when discussing business with individuals you haven't spoken to before.

Keeping Small Business Safe

Each of these targets and attacks are just some of the most popular and hard-hitting attacks out there now. The list is forever changing, and the methods we use to protect against them always needs to change too.

Some can be defended against with great security, backups, and software. Others, such as social engineering, need you and your staff to stay up-to-date and remain vigilant about the major attacks affecting small business today.

If you need help tightening your businesses security, give us a call at 281 318-1680.

Make IT Problems Last Year's Problems

Around the world, the new year is a time for celebration. It's a time to reflect and a time we typically resolve to make the most of coming 12 months. We do this by leaving last year's problems precisely where they belong, in the past year.

Many manage to adopt this approach in their personal lives, but it pays enormous dividends to apply it to our businesses too.

Cleaning up open issues from previous years gives you and your team free reign to make the next year a record-breaking success with nothing to hold you back. Intermittent IT problems, network slowdowns, printing issues, and unavailable resources can all be left in the past.

Starting the year off with a clean IT slate simply leaves you to handle the business areas which you do best.

Set Your Network Straight

If your only relationship with IT last year involved calls to fix broken systems then it is time to have your IT fixed up for good. Break-fix relationships can add stress to both your company and your IT provider.

While getting up and running fast and fixing breaks to get back on track is a clear priority, more can be done to ensure breaks don't happen and downtime is avoided. Repeated break-fix call outs waste large amounts of time to troubleshoot, diagnose, and patch an unfamiliar system every time it has an issue.

Using IT to set you up right means using knowledge and experience gained over time to right the ship and keep the whole system working together.

The same experience configuring your network top to bottom can be called on again to update or change it as requirements and projects shift. With a complete system picture, less time can be spent on troubleshooting, and more can be allocated to just getting work done.

Sports Car IT

IT with long-standing issues and bugs, ones that staff have gotten accustomed to working around, can be like running an old vehicle. It's often more expensive to maintain an old car than purchase something more modern requiring less maintenance. An old car requires more parts, becomes less efficient, uses more oil, and is more likely to suffer breakdowns too. The same is true of old IT.

The cost over time of a well-configured system can often be the same or even less than fixing broken issues on the old one. The difference is a dramatic difference in downtime and lost productivity. Better IT means getting where you need to be, faster.

Your Staff Deserve IT

Nothing distracts employees from a task more than unexpected downtime or systems failures. Whether getting crucial documents Friday afternoon, or attempting to settle into work Monday morning; bad IT is frustrating, disheartening, and time-consuming.

One of the hardest but most rewarding elements to cultivate in a company is good staff morale. When you have it, productivity goes up, turnover goes down, and the business environment is vastly improved for everyone. When you don't have it, the workday is that much tougher for everyone.

Workflow issues are well known to be one of the top contributors to poor morale. Slow machines, unavailable printing, and interruptions cause more knock-on issues than just the IT department can fix. Good employees need and deserve the right tools for the job.

A Better Way to Operate

Use the new year as a golden opportunity for a fresh start on your IT. An assessment of your system by IT professionals will diagnose issues and give you a complete guide to get back on track. Whether caused by a configuration error, bad devices, or something else; we'll track down the causes and leave them to be forgotten about.

There's never a better time to establish a managed IT services relationship. Contracting professional services can put an end to system bottlenecks, configure your system right, and advise on the best course to take into the new year.

The most important decision you can take into the year ahead is to stop addressing IT issues as they happen. Take charge of your IT and fix the underlying causes holding you up.

Give us a call today at 281 318-1680 to start a service relationship that will see your business take off into a very happy new year.