

Five Things Small Business Owners Need To Know About Identity Theft



Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

We often hear about issues with personal identity theft, and the havoc it can wreak on your credit and reputation. Less discussed,

though, is small business identity theft, and how it can affect your company. Here are five things business owners need to know.

Small businesses are liable for their bank accounts

If someone steals money out of your personal account, chances are your bank is going to cover that. But if a small business account gets drained, small business owners are on their own.

Banks typically won't cover these types of losses. Sometimes, a computer crime endorsement on your business insurance policy is available, and may cover some of your losses. With nearly all banks offering online access to account

information, experts recommend you regularly monitor your accounts.

Most hacks take a year or more to discover

In nearly all cases, it's going to take over a year for a business owner to discover they've been hacked. Too many business owners take the stance of "wait and see," assuming if they don't see anything wrong, everything's okay.

The fact is, nearly all hacks targeting small companies are stealthy - the truly effective ones don't announce their presence.

Security assessments don't find human mistakes

In many cases, the security assessment process is broken. Consider this example: A government contractor is working remotely at a coffee shop. The user left his system to visit the restroom, leaving his screen visible.

The confidential information, accessed through a secure VPN, was open and accessible while he was away. Assessments don't find these kinds of breaches, although they happen every day.

The good stuff is in the trash


Hacking can be low tech, too. Someone ravaging through a trash receptacle outside your office can use unshredded documents, mail, and other items to convince banks and other creditors that they are the legitimate business owner.

Once the bank is on board, criminals can take out loans and open other accounts using the business owner's identity.

60% of identity theft happens at the small business level

Studies show that more than 60% of identity theft cases involve a small company or small company owner.

Fifty percent of these hacked companies will go out of business either from the financial damage done by the theft, or the disclosure and negative publicity once they disclose the breach (which is something they most likely will have to do, particularly if the breach involves credit card or health information). If you don't disclose it and the media gets word - the damage to your business' reputation multiplies.



Fifty percent of these hacked companies will go out of business either from the financial damage done by the theft, or the disclosure and negative publicity once they disclose the breach.

We're proud to partner with the computer industry's leading companies:



Microsoft Partner



Microsoft
Small Business
Specialist



Business
Partner

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.



Strategically Upgrading Your Computer Systems

“The best way to make sure that your systems are prepared to handle the threats that are found in today’s computing environment is to make upgrading your technology a priority for your organization.”



Michael Menor is Vice President of Support Services for Tech Experts.

With technology growing faster than most businesses can keep up with, organizations have to continuously upgrade their solutions in order to maintain a semblance of modernity. The only issue with this is that many businesses can’t keep up, simply because they don’t have a team that’s dedicated to this important task.

What technology upgrades should be made a top priority and why?

Naturally, the first thing you need to know about workstation and technology updates is that you need to integrate them periodically in order to ensure optimal security for your organization.

Most viruses and malware will attempt to take advantage of weaknesses in your infrastructure in order to infiltrate it.

These weaknesses in your software and operating systems’ source code will ultimately allow these threats to force their way into your network, putting any contained information at risk.

These flaws are often addressed in software patches and system updates issued by the software developer, but tackling the updates in a timely fashion is a whole other monster.

Managing all software updates is easier said than done, especially without a dedicated IT department

watching over your technology. Regular maintenance is often pushed to the back burner and dangerously close to being forgotten about.

Therefore, the best way to make sure that your systems are prepared to handle the threats that are found in today’s computing environment is to make upgrading your technology a priority for your organization.

Software Updates

There are several programs that your organization needs in order to stay functional, so your software updates aren’t limited to just your workstations’ operating systems.

The fewer unnecessary security flaws that can be found in your IT infrastructure, the safer your information will be.

Furthermore, users who are working with top-notch, optimized technology will be far more productive than they would be if they were using sluggish, bogged down computers.

It doesn’t make any sense to let your employees use machines that hold them back from achieving their maximum productivity.

In fact, sometimes you might encounter a situation where using a different software will be better for your business strategy.

It’s always recommended that you consult with a professional technician before making drastic changes to your business’s software infrastructure.

Antivirus Updates

Your antivirus solution is often a

software solution, but virus and malware definitions are continuously being updated.

If your antivirus and other security software solutions aren’t properly maintained, it’s like you’re “leaving your keys in the front door,” so to speak.

Your antivirus solution needs to be managed on all workstations – or, better yet, centrally controlled from the server to ensure that all users are protected and up to date at all times.

Hardware Updates

Older hardware that’s been around the block a time or two might have proven reliable, but it will eventually start to show signs of its old age. Hardware failure becomes more likely and you run the risk of losing information due to the degradation of your technology.

This is why monitoring your systems for faulty tech and periodically upgrading to more recent models is preferable, if not necessary.

Granted, all of these software and hardware upgrades may feel overwhelming. This is why Tech Experts offers a remote monitoring and maintenance solution that’s designed to administer patches to your mission-critical systems remotely.

This helps your organization ensure that your systems are always up-to-date. We can also monitor your infrastructure for any irregularities that might be caused by hardware malfunctions, hackers, and much more. Call us at (734) 457-5000, or email info@mytechexperts.com to learn more.



Pros And Cons Of Cloud And Physical Backup Solutions



Scott Blake is a Senior Network Engineer with Tech Experts.

When it comes to backing up data, you have two choices – you either maintain physical copies of your data or you utilize cloud services to host your data. Before you make a decision, you should look into the pros and cons of each and determine which one is a good fit for you.

Pros of Cloud-Based Services

1. Utilizing the cloud requires no capital investment for additional hardware or personnel to monitor and maintain your data locally.
2. Cloud service providers offer scalability to your data needs. No more adding additional drives or servers to maintain your data.
3. Data stored in the cloud is safe from any disasters that your office may have.
4. Your data can be accessed from any Internet connection in the world.
5. No maintenance of data drives. The cloud service provider takes care of everything on their end.
6. Cloud-based storage for your data will remove any risk of

data corruption or hardware fault. This will allow you to reduce overhead by reducing the amount of IT staff personal assigned to manage and maintain your company’s data.

Cons of Cloud-Based Services

1. Cloud storage requires an Internet connection for uploading and downloading of data. If your connection is slow, you should expect slower uploads of data and increased access time to your data.
2. While almost every cloud service provider offers plans that come with data encryption, not all do. Make sure your cloud provider is securing your data.

Pros of Physical Backup

1. No vendors to deal with. You are in complete control of your data. You control how it’s backed up, accessed and maintained.
2. Data backups tend to take less time. There is no dependency on an Internet connection for backing up or accessing your data.
3. You are in complete control of the security process that protects your data.

Cons of Physical Backup

1. Localized data storage does offer the sense of control and

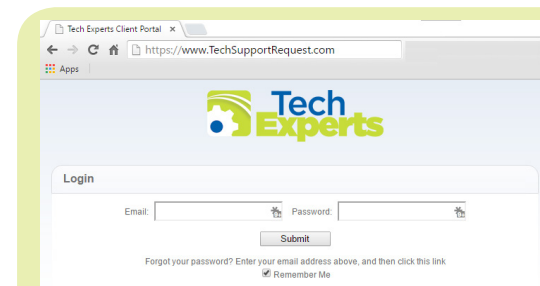
knowing where your data is. However, that piece of mind can incur some high costs and overhead.

2. As the size of your data grows, so does your investment in storage media such as flash drives, external hard drives, internal hard drives and additional servers.
3. Physical devices will fail. It’s not “if,” but “when.” All mechanical devices will fail at some point in their life cycle. Additional IT staff will need to be put in place to monitor and maintain the physical equipment to ensure data integrity. This increases overhead.
4. In the event of a disaster in your business, data accessibility and recovery will be dependent on if extra steps were taken to secure physical copies of your data off-site.
5. Doing this will require the purchase of additional hardware and additional manpower to ensure the data is corruption-free.

Again, before deciding which method to implement, figure out which solution will work best for your business. Not every company’s backup or data storage needs are the same.

For assistance in setting up either cloud-based or local backup solutions, call the experts at Tech Experts: (734) 457-5000.

“Before deciding which method to implement, figure out which solution will work best for your business. Not every company’s backup or data storage needs are the same.”



Create new service requests, check ticket status, and review invoices in our client portal: <http://www.TechSupportRequest.com>



Contact Information

**24 Hour Computer
Emergency Hotline**
(734) 240-0200

General Support
(734) 457-5001

(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001

(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!

Log on at:
www.TechSupportRequest.com



**TECH
EXPERTS**

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Have A Disaster Recovery Plan? Consider An Update

Much of one's vital information may be stored digitally that its loss could be potentially devastating.

Although we all know the value of backing information up, it's often not performed as regularly as it should be, in reality.

Think about how you and your business would cope with a natural disaster or hardware malfunction that wipes all of your precious data. Do you have a plan in place to recover it?

Chances are, you do have a recovery plan: it may be shooting your files into cloud storage or backing your data up periodically on USB

drives or other external storage.

While such plans are certainly better than nothing, they may not be the current best choice for your needs.

After all, the potential threats to your data security are constantly changing and growing, and in order to protect yourself and your business files, your disaster recovery (DR) plan needs to evolve, too.

Your computer systems and hardware have also likely evolved since the last time the DR plan was created or updated. These changes can greatly impact the efficacy of your current DR plan.

Just as your software needs occasional updating, your recovery plan also needs periodic tweaking to best protect your data.

Set up a schedule to review and adjust your plan regularly, and always give it some extra care when your business undergoes a significant change. You may even consider testing your current plan to identify its strengths and weaknesses.

The important thing, however, is that your business does make updates to how you intend to deal with disaster, so those hurdles can be overcome with as little headache, downtime, and cost as possible.

Windows 10 Updates Are Now Mandatory

For those who have made the switch to Windows 10, there are some changes to how the new operating system updates are handled.

While users were previously notified of the availability of updates and were prompted to install them, these changes are now made automatically. Most Windows 10 users are likely unaware of this change because the only notification from Microsoft is a brief line in the licensing agreement that states users will "receive automatic downloads without additional notice."

Microsoft doesn't have any nefarious intentions (or at least we hope they don't) by making this change; its intent seems to keep the most up-to-date version of the operating system on users' devices.

There are, however, some potential drawbacks to having automatic updates without user knowledge.

While the updates make it easier for Microsoft to keep up with changing technology, knowing its users are basically all on the same page and developers have a consistent target audience, these updates can potentially cause systems to interact differently with other hardware devices that aren't part of the updates.

A particular printer's driver, for instance, may lose functionality with an automatic update, and affected users would just be dumbfounded as to what happened, ultimately having to replace that hardware device.

Although Microsoft isn't making any settings changes widely known, there is a way

to configure your device to only install security updates automatically. This keeps your PC or tablet safe from the latest security threats while keeping your computer system as stable as possible.

Unfortunately, this option is not available to users running the Home version of Windows 10. Thus far, only the Enterprise Edition provides this capability, which is an important consideration for business owners.



"You put the wrong kind of ram in my computer!"