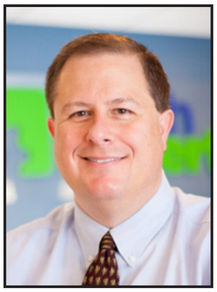
December 2018

TechTidbit.com
brought to you by Tech Experts

Data Encryption – What You Really Need To Know



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

In today's digitally driven world, far too many personal and business devices are left unsecured. These devices don't leverage strong passwords and fail to have the encryption needed to protect vital data.

Whether companies choose to store data in public, private, or hybrid clouds, they should always ensure that the data is encrypted before it leaves their devices or networks.

Additionally, when employees think that "this data isn't important," they are creating the weak links that hackers need to successfully infiltrate a device (or network) and subsequently steal unencrypted data, upload malware attacks, and otherwise wreak havoc on unsuspecting businesses.

Why Should Businesses Encrypt Devices?

The primary reason that businesses need to encrypt all devices is due to the sensitive data that they hold. Take, for example, Amarillo, Texas which said that one of the companies in charge of a security payroll audit for the city lost a flash drive containing city employees' names, bank deposit information, birthdays, social security numbers, and addresses.

Secure Device Configuration

When devices are not correctly configured, then it doesn't matter if your company has robust security protocols. With this in mind, securing devices is made easier when your business follows these vital steps:

- Lockdown any services, including remote management systems, that you are not using.
- Disable and/or change the default settings on ports.
- Prohibit the use of outdated web technologies. In this vein, Java, NPAI, and Plugins need to be kept up to date to avoid any potential security vulnerabilities.
- Create strong passwords.
- Leverage encryption for any and all business data and devices.

It is important to note that you must complete all of the above steps. For example, if you use a strong password, but fail to properly encrypt your device, then it could still be subject to theft or hacking attempts.

Fortunately, there are three additional steps that you can take to further protect your vital business data and devices.

3 Steps To A Strong Configuration

Securing your essential business data is made easier when you complete the following three steps.

1. Strong Passwords And Encryption — Did you now that in 2017 81 percent of hacking-related breaches were due to stolen (or weak) passwords? In this vein, you must ensure that your employees are following password best practices. It is especially crucial that sensitive data sent via email or stored on the cloud is appropriately encrypted.

2. Endpoint Protection — Endpoint protection will require you to complete plug-in and browser updates, use an up to date anti-virus software, and implement a proven use Data Execution Prevention (DEP) and use Endpoint Threat Detection and Response (ETDR) that has been customized for your business needs.

3. Restrict The Number Of Login Attempts — When an employee has an infinite number of login attempts, then their "strong password," is made null-and-void. Instead, you should limit the number of login attempts to business devices or networks.

As an added level of protection, you should ensure that employees can only access portions of your system from approved devices.

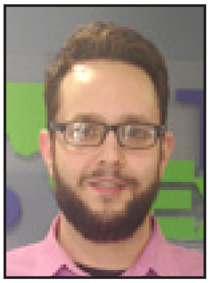
The Bottom Line: Take The Steps Needed To Encrypt Data And Devices

If you want to ensure that your business data, devices, and networks remain secure, then you need to use the proper encryption methods.

Through endpoint protection, a restricted number of login attempts, secure passwords, and encryption best tactics, you can keep your vital business data safe from hacking attempts.

When employees think that "this data isn't important," they are creating the weak links that hackers need to successfully infiltrate a device (or network) and subsequently steal unencrypted data, upload malware attacks, and otherwise wreak havoc on unsuspecting businesses.

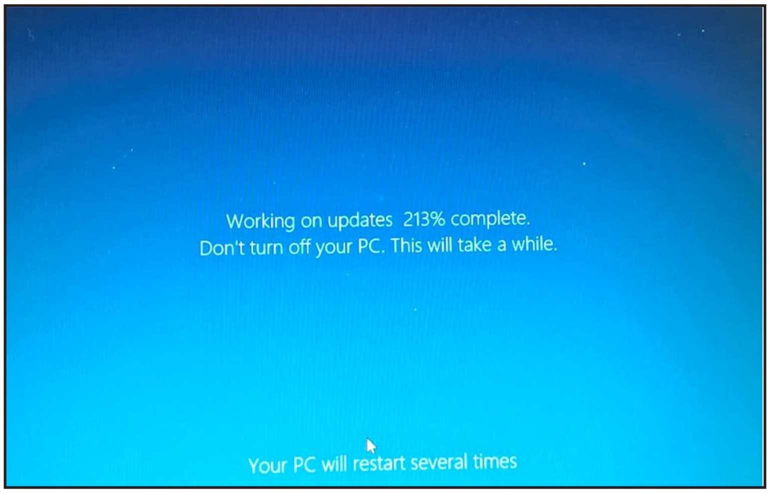
Back At It Again: Microsoft Suspends Windows Updates



Jason Cooley is Support Services Manager at Tech Experts.

Windows 10 was released in July 2015 and there were plenty of reasons to be excited. If you have been around for the last few versions of Windows dating back to Vista, you may have a love/hate relationship with Microsoft.

Windows Vista, for instance, was once known as the biggest failure Microsoft had experienced. That is, until Windows 8. Just using the adoption numbers, it's clear that Windows 8 was the least successful OS that Microsoft has ever released.



Working on updates 213% complete.
Don't turn off your PC. This will take a while.

Your PC will restart several times

So, Microsoft and their users had many reasons to be excited about Windows 10. Microsoft assured users that Windows 10 would be a return to the golden standard of Operating Systems: Windows 7.

As with all releases of a new operating system, there have been some issues. Some of these problems are indicative of a bigger problems while others are standalone issues.

With a myriad of different types of problems that have surfaced over the last couple of years, Windows 10 may be the most problematic OS of all-time.

Since launch, Windows 10 has had some very unusual problems. While it is almost expected for issues to arise with a new OS, the frequency and type of problems is what's disturbing. The issues have ranged from broken drivers that leave devices nonfunctional to our latest and greatest issue: the deleted documents folder.

A few times a year, larger updates called "Feature Updates" are released. In April 2018, there was an update that would incorrectly create a duplicate of your documents folder. A lot of these folders were empty and had no real purpose.

At this point, Microsoft decided to implement a fix with their next feature update, due in October 2018. The "fix" would remove the duplicate folder.

There was one very large issue with this. The update did not check if the folder was actually empty before deleting it from your system. People all over began reporting the issue where, all of a sudden, their files were gone.

Once reported, Microsoft acted quickly to halt the update before further systems were affected. The update would still download but would not apply. It was necessary that the access to the update be stopped to save additional systems from data loss.

A strange side effect of the update being put on hold was the failure to apply the downloaded Windows updates.

This resulted in much longer shut down/restart times as the update would attempt to apply, then roll back once it failed. This also provided users with another reason to be frustrated.

The issues are now resolved. The fix has been implemented and there is no more possibility for further data loss.

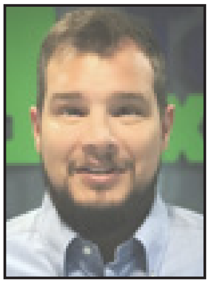
For what it's worth, Microsoft also asked for users who lost data to reach out, and they would try to recover it where possible.

It seems like the least they could do considering the issue was created due to poor planning, poor programming, or some combination of those.

When possible, look into deferred updates. Let the problems work themselves out before taking on the unnecessary problems.

> *"Since launch, Windows 10 has had some very unusual problems. While it is almost expected for issues to arise with a new OS, the frequency and type of problems is what's disturbing. The issues have ranged from broken drivers that leave devices nonfunctional to our latest and greatest issue: the deleted documents folder."*

Crypto Blackmail: How To Protect Yourself



Frank Deluca is a field service technician at Tech Experts.

A criminal contacts you over email or snail mail and insists they have a webcam video of you watching "unsavory" videos or evidence you cheated on your wife.

To stop the release of this compromising information and to make the problem go away, the criminal asks for digital payment in Bitcoin or another form of cryptocurrency.

You should never respond or pay. All the criminals have are empty threats and they're just trying to trick you.

What is CryptoBlack Mail?

CryptoBlackmail is any sort of threat accompanied by a demand that you pay money to a cryptocurrency address.

Just like traditional blackmail, it's a "pay up or we'll do something bad to you" threat. The difference is the demand for payment in online currency rather than traditional hard (and traceable) cash.

Why cryptocurrency? It's not possible to "undo" a transaction and it's hard for the authorities to track down the owner of a Bitcoin address.

With cryptocurrency, the money is gone as soon as you send it.

Some examples of CryptoBlackmail:

- Physical mail saying "I know you cheated on your spouse," and demanding payment in the form of Bitcoin to a specified Bitcoin wallet.

- Emails claiming an attacker has placed malware on your computer and recorded you in a uncompromising position, along with a video feed from your webcam. The attacker also claims to have copied your contacts and threatens to send the video to them unless you pay.

- Emails including a password to one of your online accounts along with a threat and demand for payment to make the problem go away. The attacker just found your password in one of the many leaked password databases and hasn't compromised your computer. Keep in mind that the criminals almost certainly cannot follow through on their threat and they probably do not have the information they claim to have. It is simply a numbers game.

For example, someone may just send emails saying "I know you cheated on your spouse" to a large number of people knowing that, statistically, some of them will be tempted to act.

The important thing to note is that this not a personally targeted attack. Unfortunately, the scammers do trick some people, which then perpetuates this ongoing CryptoBlackMail scam as an easy payday for criminals with little to no work involved.

How to Protect Yourself

Ignore the scammers. Delete and forget the scam. Don't try to negotiate or even respond with the scammer. Don't pay a single cent.

Don't re-use passwords. If a criminal sent you one of your passwords, it's likely that password was from one of many leaked password databases available online.

Change your passwords. If you're concerned a criminal might have your passwords, you should change them immediately.

Get a password manager. They can help keep track of those unique passwords. They remember passwords for you, letting you use strong, unique passwords everywhere without having to remember them all.

Disable your webcam. If you're really worried about someone spying on you with malware on your computer, you can just disable your webcam when you aren't using it.

The most important thing to do — aside from never paying the scammers — is to ensure you aren't re-using passwords, especially if they've already been leaked. Use strong, unique passwords and you won't have to worry about password leaks. Just change a single password whenever there's a leak and you are done.

> *"CryptoBlackmail is any sort of threat accompanied by a demand that you pay money to a crypto-currency address. Just like traditional blackmail, it's a "pay up or we'll do something bad to you" threat. The difference is the demand for payment in online currency rather than traditional hard (and traceable) cash."*

Contact Information

24 Hour Computer
Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(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) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Are Smartphones And Tablets Killing The Traditional PC?

In the early days of the Internet, there was only one device that enabled you to access it. That was the desktop computer.

Laptop computers have existed for as long as desktops have, but due to hardware limitations, they never really became a viable alternative.

In a technical sense, laptops are "mobile" devices, but still require the user to be seated to use. It hasn't been until recently that we have seen truly mobile devices.

The Rise Of Smartphones

The first smartphone was invented in 1992, three years before the term "smartphone" even existed. It was IBM's "Simon," which was a cellphone with a monochrome LCD touchscreen and a stylus.

It was the first phone was able to send faxes, pages, and emails and it was even capable of running third party applications.

It came with built-in features that are so commonplace on today's smartphones that most people take them for granted, such as a calendar, a notepad, a world clock, and a way to schedule appointments.

Simon didn't sell well and its $899 price tag surely didn't help move units either. For comparison, that's the same purchasing power as $1607 in 2018.
It wasn't until Apple's iPhone in 2007 that the modern smartphone became mainstream. IBM was able to sell a total of 50,000 Simon smartphones over its entire lifetime, a number that is dwarfed by Apple's 1.4 million iPhone sales in the first year of its existence.

The Aging Desktop

Hardware advancements in recent years have made smartphones powerful enough to perform all the basic functions that consumers were using desktops for in the early days of the Internet.

Smartphones are also priced lower than their desktop counterparts. Sure, if you compare the price of a brand new, top-of-the-line smartphone to a much more powerful desktop PC you may find that the desktop by itself is less expensive.

But for a desktop to function you also need peripherals like a monitor, keyboard, a mouse, speakers, etc. You also need a desk, a chair, a constant source of power, and, in most cases, an entire dedicated room. One could make the argument that you need to pay for a cell phone service to be able to use all the functions of a smartphone, but that isn't much different than paying for an ISP.

Tablets

In 2010, Apple made yet another mobile device that would change the tech world forever: the tablet. Tablets are essentially large smartphones although they aren't typically used to make phone calls.

Due to their size, they are capable of carrying stronger hardware than smartphones and they are easier to use as a practical tool in the workplace. There are even specialized "professional" tablets that are designed with detachable keyboards and Bluetooth mice that run the same operating systems that their desktop cousins do.

They weigh less than modern "lightweight" notebook laptops, and have the advantage of a touchscreen. Their functionality comes at a steep price though, and it's one that will be felt by your wallet. Most "professional" laptops will cost even more than the most powerful desktops and laptops.

No Clear Winner

Each option has different pros and based on how you intend to use it. Although smartphones and tablets have been quickly taking over the home user market, almost all workplaces still use the desktop computer.

The price per performance ratio is still in the desktop's favor. It could be a very long time before mobile devices gain the functionality of a desktop while matching their price.