TECHNOLOGY TODAY

FC Friendly Connections IT
STAY CONNECTED

Insider Tips To Make Your Business Run Faster, Easier, And More Profitably

November 2015

Inside This Issue…

Server Maintenance ....Page 1
Crypto Trojan review...............Page 2
Cybercrime trends ....Page 3
Humor ....Page 4
Pets after retirement ....Page 4

SplashData's latest list of the WORST passwords that people choose.

1-123456
2- password
3- 12345
4- 12345678
5- qwerty
6- 123456789
7- 1234
8- baseball
9- dragon
10- football
11- 1234567
12- monkey
13- letmein
14- abc123
15- 111111
16- mustang
17- access
18- shadow

Do you have a server?

As I'm writing this I'm doing some remote server maintenance (lots of click and wait type stuff). Servers are not PCs. Just to be clear I'm talking about actual servers running Microsoft Server 2008 or 2012 not PCs acting as file sharing equipment. If your company has a server then you are likely in a domain environment meaning you sit down at your computer and hit control/alt/delete putting a password in the window that comes up. Any company with more than five people in it should probably have a domain. It is a much easier way to safely and securely manage your computer environment by your IT support.

Servers are very different animals that need to be treated with respect. They nearly always live in a steady state environment. No one is at the keyboard, no one is downloading the latest joke or cruising Facebook. They are designed for smooth, predictable response and dependable storage. They aren't meant to be restarted every day and work better if they are left alone. Frequently ignored. As it should be—to a point.

Once a month, every server wants some attention and that's what I'm doing today. I'm on a remote server checking the logs to be sure nothing bad has happened in the past month and that everything is running well. I'm running necessary security updates (something that is not automated on servers, or should not be). I'm making sure the antivirus is updated and scanning correctly and there are no problems in that area. I've got a check list and I'm going through it. We do that with all of our business contract customers. It is one of those things that they don't see because it is done in off hours and who really reads the reports of their IT support?

It is not flashy, not sexy, not bleeding edge. But it keeps things going. Monday morning my clients will come in and log in just as they do every morning. And just like every morning things will work. How boring.

Bill Schubert

Keeping your files safe from Trojans

Cryptolocker first appeared in 2013. It was a new kind of Trojan – an ordinary-looking file that, when opened, releases malware into your computer.

Cryptolocker's twist was that it would encrypt all the files on your machine and demand a ransom to decrypt them. It also displayed a timer and if you didn't pay before it ran out your files would be gone forever.

The good news is that in June 2014, an international team of cybersecurity experts was able to neutralize Cryptolocker and indict the head of the crime syndicate responsible for it. The bad news, however, is that other criminals had already started work on copycat Trojans.

Now "CryptoWall" and "TorrentLocker" are making the rounds, forcing many business owners to choose between financing illegal activity and surrendering valuable data. So what can you do to protect yourself from these programs?

Prevention is better than cure

Unfortunately, there's no "cure" for CryptoWall and TorrentLocker – if you decide not to pay the ransom, you're unlikely to ever retrieve your files.
So here's how you can prevent your computer or network from being attacked: both CryptoWall and TorrentLocker spread using false attachments that usually arrive with unsolicited emails from government departments. To stay safe, it's a good idea to introduce rules on how to treat unwanted emails.

You should also take steps to limit damage in case of an infection. The biggest mistake you can make is to have an attached drive being used as a "backup". If the drive has a drive letter then it will do no good. It too will be encrypted. The same holds true for Dropbox and other syncing software that had a drive letter on your PC. And of course you should **always also use a strong and regularly updated antivirus program with active scanning like AVG CloudCare.**

Back up regularly

Backing up you files is the most important step you can take towards protecting yourself from ransomware. With regular backups, you can restore important files even if your network or computer is compromised. However, it is vitally important that you back up your files to an external source. Otherwise, a Trojan like Cryptowall might encrypt your backup files too.

Consider your cloud solution

In July 2015, Heimdal Security reported that CryptoWall 3.0 had begun to spread to files stored in Google Drive, the popular online storage service. At around the same time, Cryptowall was also detected in Dropbox. Many users were shocked to learn that they couldn't retrieve their files from these sites – and that's why it's so important to distinguish between file syncing and file backups.

If you've moved to the cloud, ensure you're using best practice backup procedures. And if you're committed to Google Drive, consider a service like Backupify which automatically copies your files on Google Drive to a secure location.

Keeping ahead of the crypto-villains

According to the FBI, CryptoWall infections cost American consumers US $18 million dollars between April 2014 and June 2015. Make no mistake – they're dangerous programs and can paralyze your business if you're unlucky enough to open the wrong attachment. So be proactive, educate your colleagues, and make sure that your files are kept out of harm's way.

Know your enemy: three new trends in cybercrime

Cybercriminals never stop trying to come up with new ways of cracking your passwords and stealing your data. It's a constant game of cat-and-mouse, and it’s vital to stay informed about the latest trends and scams. Here are three to look out for.

1. The fake attachment

It’s one of the oldest tricks in the book, but according to Proofpoint’s June 2015 half-year threat report, the first few months of the year saw a spike in the number of emails sent with fake attachments – usually files that appear to be documents but contain hidden malware.
In May, for example, hackers stole more than a million records from the Japanese Pension Service after one of its employees accepted an attachment that arrived with what they thought was an email from the Ministry of Health.

The lesson is clear – be very careful when opening unexpected attachments, and never open one from an unknown sender. Wherever the attachment comes from, you’d do well to scan it first with a good anti-malware program.

2. The request for confirmation

With LinkedIn and Facebook’s combined "population" more than twice that of continental Europe, criminals can generally assume that the CEO, CFO and senior managers of a target company have online profiles floating around somewhere.

Using the information in those profiles they can then set up a convincing fake email or social media account. They can send emails, or even voice messages, from the manager they’re impersonating to lower-level staff requesting that they confirm sensitive information, like passwords or security procedures.

Fortunately, it’s easy enough to prevent this form of cybercrime by implementing internal identity authentication procedures (like two-factor authentication or even biometrics) and using email filters to block messages from "lookalike" addresses.

3. The social media scam

Some cybercriminals are creating tailored social media advertisements that take users who click through to online scams, or trick them into downloading viruses and malware.
As Proofpoint notes, “a single phishing lure, malware link or spam message posted to a high profile corporate social media destination may be viewed by ten thousand or more potential victims.” For example, Facebook is routinely flooded with false NFL-related content designed to look completely authentic. When it comes to your business, ensure any social media log-ins are carefully protected, and be sure to report any content that uses your brand to dupe customers.

What’s the prognosis?

According to the a report by Juniper Research, the global cost of data breaches is likely to hit US $2.1 trillion per year by 2019, with the average breach costing US $150 million. What’s worse, North America currently tops the list of likely targets – in 2014, for example, the FBI received an average of 22,000 cybercrime-related complaints a month.
In this environment, no business can afford to experience "breach fatigue" – the state of being so "numbed" by constant cyberattacks that you become careless about security. Instead, you must stay vigilant, install reputable security programs, and keep track of new trends in cybercrime. That way, you can keep your business safe, and your customers too.

Unruly Child

A man scolded his son for being unruly. The child rebelled.

He got some of his clothes, his teddy bear and his piggy bank and proudly announced,
"I'm running away from home!".

The father looked at the matter logically.
'"What if you get hungry?"
"Then I'll come home and eat," bravely declared the child.

"And what if you run out of money?"
"I will come home and get some!" readily replied the child.

"What if your clothes get dirty?"
"Then I'll come home and let Mommy wash them," was the reply.

The man shook his head and exclaimed, "This kid is not running away from home, he's going off to college."

"I just read an online article that says you should never believe anything you read online."

Pets after retirement

They can bring joy to your life. As we get older, pets help us stay active and provide companionship. Studies even show that petting a dog increases levels of oxytocin, called the love hormone.

Animal companionship has been associated with decreases in fatigue, loneliness, stress and social isolation, common conditions to which older adults are vulnerable.

When you think of adopting, check out the animal shelter first. Dogs who aren't pedigreed are often healthier than those who have expensive pedigrees, but there are plenty of pedigrees that end up at the shelter.

If you can't walk a dog, consider getting a cat. They require less care and can be great companions. Some people like birds or fish for pets, but they can't follow you around the house.

Remember that puppies are cute, but require more work, and their energetic play could wear you out. A two- or three-year-old dog is better.

Small dogs are popular choices for retirees. These breeds are very small. Most weigh less than 10 pounds. All are lovable companions but will bark when someone comes to the door.

- Maltese are are fun to maintain, are up to 10 inches tall, hypo-allergenic, don't shed, and are very loving.
- The Chihuahua may live up to 18 years. They weigh about 6 pounds, are lovable, very smart and easy to train.
- A Yorkshire Terrier weighs 4 to 6 pounds and is up to 9 inches tall. It's the most famous of the small dog breeds.
- The Pomeranian, called the teacup dog, weighs up to 7 pounds, loves to take walks, makes a great indoor dog.
- Cavalier King Charles Spaniel is one of the friendliest breeds, often used as a therapy dog, and is very loving.

EDITORS NOTE: I just put this in so I could add the picture. It was worth it.