MC Connect

"Insider Tips to Make Your Business Run Faster, Easier, and More Profitably"

Why Do Bad Guys Write Viruses, Anyway?

The other day I was meeting with a prospective client and the subject of security came up. I don't remember all of the details, but I'm sure I am the one who brought up the topic because it's something I'm passionate about. I was met with casual dismissal. Actually, I'm not sure if casual is really the right word. It was almost contemptuous.

"I don't care about that! My company is too small. They go after the big guys, not organizations like mine."

I think what surprised me most about this conversation is

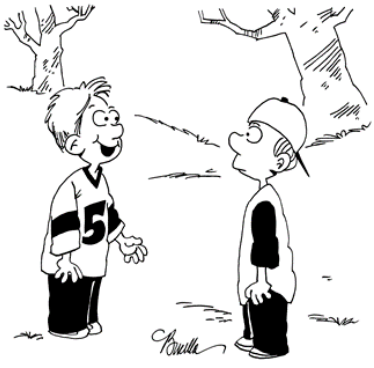
"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

- Justin Shelley, Master Computing

March 2015

DENTON, TEXAS

Inside This Issue…



"You know what I just noticed about playing outside? No pop-up windows."

Master-Computing.com
connect@master-computing.com
940-220-7817

MASTER COMPUTING

that his response didn't, in fact, surprise me. It wasn't until later that I realized how often I run into this type of attitude, and how fatal such an attitude can be. Sometimes the conversation is about network equipment such as firewalls, sometimes we are discussing security updates and patches, sometimes it's PCI or HIPAA compliance procedures, and sometimes we're talking about "nuisance" spam and viruses. Regardless, it all ties back into a general lack of give-a-crap that can only be based on ignorant bliss. Oops… Did I say that out loud?

To be fair, we all have finite resources (time, money, mental energy), so we simply cannot focus on everything that demands our attention. Cybersecurity (the process of applying security measures to ensure confidentiality, integrity, and availability of data) is one of those "necessary evils" which doesn't always seem so necessary at all. We hear stories about security breaches at large organizations, like Target, for example. But how often do we hear stories about small businesses getting hacked? Almost never. Why? Because it doesn't happen? Nope! We don't hear about those stories because they happen so frequently that they can hardly be considered newsworthy.

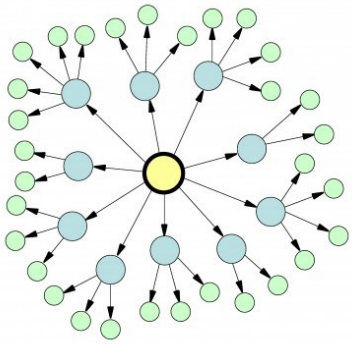
When meeting with clients, there are two phrases we hear almost constantly: "Oh, I probably have a virus or something" and "Why do people write viruses, anyway?" The first phrase is said as a way of dismissing the problem. It's "only" a virus. It is a nuisance, but I've learned to live with it. What?!? If only they knew the answer to the second phrase/ question; the *why* behind viruses. If we really understood *why* people write viruses, perhaps I would never again hear the first phrase or any of its variants, like "It's only a virus." So why *do* people write viruses? And let's go ahead and couple that with, "Why do I get so much spam?" I don't have the space here to do this topic justice, but if you are really interested, grab a copy of Brian Krebs' new book, *Spam Nation: The Inside Story of Organized Cybercrime, from Global Epidemic to Your Front Door*. Here is a very high-level overview:

Bad guys need money, just like the rest of us. Bad guys have found a few easy ways to get money from us unsuspecting, law-abiding citizens. We'll look at just two of those: they can steal it directly from our bank accounts, and they can trick us into buying inexpensive, discreet prescription medications. Seriously. People do actually buy those little blue pills from unknown "online pharmacies" run by underground criminals. Those spam emails are in your inbox because they WORK! Millions of people buy those pills. I shouldn't have to say this, but please don't buy *anything* from *anyone* who sends you an unsolicited email. Ever.

What does this have to do with you? And why are we talking about blue pills instead of viruses? I'm glad you asked. You see, bad guys have to advertise their services just like you and I do. They do this via spam. But people hate spam, so everyone gets mad at the bad guys. With enough effort, we sniff out the bad guys, find out where their spam-sending Viagra-peddling servers live, and we shut them down. For a while, that worked. A very short while. Then the bad guys, mad because we took away all their money-making servers, found a new way to email us about Viagra. They learned that they could make YOU send out all their Viagra ads on

their behalf. So they wrote a program to accomplish that very act. And we call that program a “virus”.

A virus-infected computer is really a single soldier in a massive global army led by underground thugs. These global armies of compromised computers are called botnets, short for ro**bot net**works. That nuisance virus that you’ve learned to live with is slowing down your computer because it has commandeered your resources (processor, memory, and Internet connection) to help send out the billions of emails that plague our inboxes every day.



But wait, there’s more! Since these underground thugs now have complete control of your computer (as well as millions of other computers), why on earth would they stop at *only* sending spam? Why not also steal the username and password to your bank account? Why not use your computer to steal corporate trade secrets? Why not use your computer to help crack encryption keys and hack into other networks? Why not use it to participate in DDoS attacks which have been known to take down entire nations? (Just google “2007 cyberattacks on Estonia”)

That “nuisance” virus that keeps us from working efficiently is doing untold damage behind the scenes. We truly live in ignorant bliss. Efficiency and productivity is at stake. And I have no interest in minimizing that issue. It is a real cost to business.

But would I be going too far to say that our national security is also at risk here?

I wouldn’t be going too far at all. At least, not according to the White House. On May 29, 2009, President Obama said, “For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation.” If you want to read the whole thing, google “Obama Cyber Security 2009”.

I have to assume that if you are still reading this article, I have your attention. And if I do, in fact, have your attention, I can guess with almost certainty that you are asking, “What now?”

Conveniently, and self-servingly, I have run out of room. So you’ll have to give me a call for the answer to that question. I would be more than happy to sit down with you one-on-one to discuss how you can face these threats head-on both personally and in your business. But let me close with one last pointed reminder that “ignorant bliss” is NOT the answer.

Justin Shelley

Luck Is For Leprechauns — Is Your Business Prepared for Future Security Threats?

If your business hasn't been the target of malicious intruders or cybercriminals, consider yourself lucky. Hackers are a relentless bunch and they want your gold: information and access they can use to exploit loopholes in your business's Internet security. The last few years have been hard on companies all across the globe. And these cyber-breaches aren't going to stop simply because the "damage has been done." In the US and Canada, reported incidents have affected over 215 million consumers and over 7 million small businesses. And that's only counting the attacks that authorities have uncovered.

For cybercriminals, there is no end game. All too often, small business owners assume they are outside the firing line and hackers aren't interested in them. While the media focuses on the big cyber-attacks, there are countless other stories playing out at small businesses everywhere. Cybercriminals are constantly in search of loopholes and weak security. And, unfortunately, small businesses often have the weakest IT security.

Security industry analysts predict that 2015 won't be much different from 2014 when it comes to cyber-security. There are going to be more data breaches. It's just a matter of where and when. It's also a matter of being prepared.

During the month of March, we are offering local businesses a FREE Cyber-Security Audit to help uncover loopholes in your company's online security. At no cost or obligation, our highly trained team of IT pros will come to your office and conduct this comprehensive audit. And after we're done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and a Prioritized Plan Of Attack for getting any problems addressed fast.

Because of the intense one-on-one time required to deliver these Cyber-Security Audits, we can only extend this offer to the first seven lucky companies who request it by March 17th—St. Patrick's Day. All you have to do is call our office at 940-220-7817 to request yours today.

Shiny New Gadget Of The Month:

The Withings Activité Pop

Lately, it seems the tech world has been inundated with wearable devices, from fitness trackers to smartwatches. They offer a number of useful features, but they also lack in elegance. They are often bulky, ordinary, complicated and—in the case of smartwatches—have less than desirable battery life.

This is where the Withings Activité Pop comes in. It looks like a classy watch on the outside, but on the inside it's a very different story. It's an activity tracker, verging on expressing itself as a smartwatch.

From the smartphone app, you control everything, from the analog dials to your activity goals. The watch face features a secondary dial that tracks your activity—from 0% to 100%—for the day. It's simple and straightforward. It's water-resistant up to 30 meters and available in three colors: azure, sand and shark gray. It's currently available at Best Buy, in-store and online.

Client spotlight: WaterTech

WaterTech is a dynamic and growing water treatment products company, manufacturing and distributing products throughout the world via a dealer network and an ecommerce store. The company has been in the water products business for over 27 years and is experiencing exponential growth in customers and products offered – everything from water softening and conditioning equipment to reverse osmosis and emergency water systems. WaterTech customers have come to expect premium products and service from WaterTech and that's what we deliver.

Located in Carrollton, TX, WaterTech has many growing tech needs. We communicate with our dealers and current/potential product end users located worldwide via phone, email, website, web conferences, chat services and our online store. In order to serve our customers, we rely heavily on Master Computing to make sure we have everything consistently online, up-to-date and working well, including:

- VOIP System
- Desktop computers and software
- Printers and scanners
- Servers
- Hardwire network
- Wireless network
- Mobile computing apps

We appreciate Master Computing's reliable, fast and competent service as we continue to grow. Bryce Linton, the president of WaterTech, explains, "With a company like ours, that's growing in staff and communication demands, it's important to have a tech partner that can discuss your needs, provide options and implement solutions that work now and also expand with you. This is what Master Computing does for us."

MARKETING THROUGH YOUR CUSTOMERS

Word of mouth—the better-than-anything-you-could-pay-for form of spreading the word about companies and products worth supporting. Your customers do your marketing for you, and you simply continue delivering the high-quality product they're raving about.

But how do you get your customers to do it?

On May 9, 2013, an article was published by a journalist who'd stopped in Dominique Ansel Bakery in New York City and asked what was new. The staff offered the journalist a taste of a new product that would launch to the public on the day after the article was published. On May 10, 2013, the Cronut™ was born. There were customers waiting outside the little bakery, lined up to sample the delectable baked good they'd read about.

By the end of the week, the line outside the bakery was 100 people long. People stood in line to sample the Cronut™ they'd heard about from their friends. And they didn't just buy one Cronut™; they bought lots of them—as well as all of the other unique, handmade pastries the shop produces.

The Dominique Ansel Bakery is a small business. They don't have a big marketing department who dreamed up the Cronut™ as a publicity stunt. They simply embrace the creativity inherent in baking, and word of mouth pulls customers from all over the world into the little shop. It's organic. It's natural. It's the power of word of mouth.

Another great example of a company whose customers are ardent fans is a well-known jewelry store (whose name I can't share with you). Their policy for purchases of engagement rings is pure genius. A couple selects a ring—say a diamond of one full carat. The jewelry store has a secret upgrade policy, and they supply the client with a stone that's just a little larger than the one they paid for. When customers take their one-carat ring to an appraiser, they discover that it's a carat and a quarter. The customer—stunned at having received more than they paid for—returns to the jewelry store, at which point the jeweler thanks them for their business, tells them about the secret upgrade and—here's the genius part—asks the customer not to tell anyone about the secret upgrade.

But the customer does tell. The customer tells everyone he can think of about the spectacular customer service he received and about the exceptional value the jeweler provided. That customer ropes in hundreds more customers, and the jewelry store doesn't do anything except make customers happy and wait for new customers to pour in. It's brilliant.

Whether customers are sharing a Cronut™ with a friend, or whether they're swearing a coworker to secrecy about the jewelry store's secret upgrade they swore not to divulge, if you can get your customers talking about you, your company and your brand, then you're starting a marketing trend that can not only become self-sustaining, but can also bring more customers than you'd ever dreamed of—right to your door.

Mike Michalowicz

FREE REPORT: If you are still relying on tape drives, external hard drives or USB devices to back up your data, then it's critical for you to get and read this informative business advisory guide.

You will learn:

1) The only way to know for SURE your data can be recovered if lost, corrupted or deleted—yet fewer than 10% of businesses have this in place.
2) 7 critical characteristics you should absolutely demand from any off-site backup service.
3) Where many backups fail and give you a false sense of security.
4) The #1 cause of data loss that businesses don't even think about until their data is erased.

Claim Your FREE Copy Today at:
www.Master-Computing.com/12facts

Master-Computing.com
connect@master-computing.com
940-220-7817

The History of St. Patrick's Day

By Jessica Shelley

Many of the traditions that we honor on St. Patrick's day, such as wearing the color green, picking shamrocks, and parades didn't originate in Ireland. Even the Patron Saint of Ireland isn't Irish. So how did all of these things become connected with Ireland? During the fifth century, a 16 year old boy named Patrick was kidnapped from Brittan and forced to be a slave in Ireland. He lived there for almost 10 years before he had a vision and was told to escape back to England. While in England he converted to Christianity, became a priest, and had yet another vision telling him to go back to Ireland to convert the people to Christianity from Paganism. There is a myth about St. Patrick that says that he drove the snakes out of Ireland. We know, of course, that this isn't true because Ireland never had snakes, but it's actually a metaphor for St. Patrick driving out Paganism.

So that explains St. Patrick, but what about green and the shamrock? Well these things are actually connected. During his ministry in Ireland, St. Patrick used the shamrock to explain the Trinity. Soon enough people started wearing shamrocks on March 17th, the day of St. Patrick's death, in a way to honor him. This eventually turned into wearing the color green. It's also said that the color green represents Ireland because of its naturally green landscape.

During the great potato famine in Ireland, many Irish people immigrated to American cities and brought these traditions with them. It was in America that parades became popular as a way to celebrate Irish culture. This holiday has since exploded and is known worldwide, but the biggest parade is still held in New York City every year.

Whether you have a claim to Irish heritage or not, I hope you get the chance to celebrate this great holiday and remember to wear green!

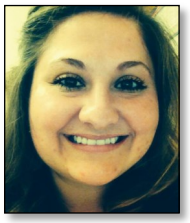
Never Forget A Password Again With A Password Manager

We all have a number of passwords for all the online services we use. You name it: banking, online bill payment, e-mail, social networks, shopping and more. You know it's incredibly easy to lose track of them all—unless you are committing one of the greatest online security offenses by using one password for everything. One of the best—and most secure—ways to handle your passwords is with a password manager.

It's not uncommon for password managers to get overlooked when it comes to online security. There is a lingering—and false—concern that keeping all of your passwords in one place can potentially open up all your protected accounts to intruders—if they are able to break into the password manager. It's a legitimate concern, but password managers use powerful encryption to keep your passwords safe. They are specifically designed to keep you even more secure than you otherwise would be.

Many password managers—including LastPass, KeePass and 1Password—do much more than simply "remember" your passwords. They also offer password- creation assistance. They will tell you if a password is too weak or just right. Some managers offer the option to generate a secure password for you. Since you don't need to remember it, it can be more complex. They are compatible with a number of platforms and they are packed with customizable tools to keep you safe.

Who Else Wants To Win A $25 Gift Card?



The Grand Prize Winner of last month's Trivia Challenge Quiz is Cassy Pruitt! She was the first person to correctly answer my quiz question from last month: **To ring in the New Year in Spain, it is traditional to do what on each chime of the clock?**
a) Eat a grape b) Take a sip of wine c) Clap your hands d) Light a candle

The correct answer was a) Eat a grape. **Now, here's this month's trivia question. The winner will receive a gift card to AMC Movie Theatres!**

According to Irish lore, St. Patrick banished all the snakes from Ireland. What other island nation is also devoid of snakes?

a) Cuba b) Madagascar c) New Zealand d) Jamaica e) Sri Lanka

E-mail Us Right Now With Your Answer!
Trivia@Master-Computing.com

The Lighter Side:

Endorse This Skill: Jihad

We endorse the skills of our coworkers, friends, acquaintances and other connections on LinkedIn all the time. But what would you do if one of your connections listed "jihad" as one of his skills? Unless you're in the business of extremism (you're probably not), you're likely to slink away quietly and alert LinkedIn admins.

Well, one senior Taliban commander decided to update his LinkedIn profile with this very "skill." Specifically, he listed "jihad and journalism." This particular terrorist leader, Ehsanullah Ehsan, even lists himself as "self-employed."

Unfortunately (or fortunately), when LinkedIn was contacted by the *Telegraph* for further information, the social media company decided it was best to take the account down.

There has been some chatter as to the legitimacy of the account. The profile's distinct lack of Taliban propaganda and recruiting information suggested it wasn't operated by the terrorist leader himself or anyone in a significant leadership position.

Of course, as a terrorist leader and all-around terrible human being, he has more pressing things to worry about other than a suspended LinkedIn account, such as a $1 million bounty placed on him by Pakistani officials.