IT² TECHNOLOGY TIMES

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

Why Choose IT²?

Technology can work in one of two ways: It can give rise to a more profitable, efficient and successful organization, or it can exhaust your resources and be a big hassle. For this reason, countless companies rely on IT² for the installation and support of the technology that powers their business.

To learn more about how IT² can help your business, give us a call today at **937.428.5880** or e-mail **AskIT2@it2resource.com**, subject line: learn more.

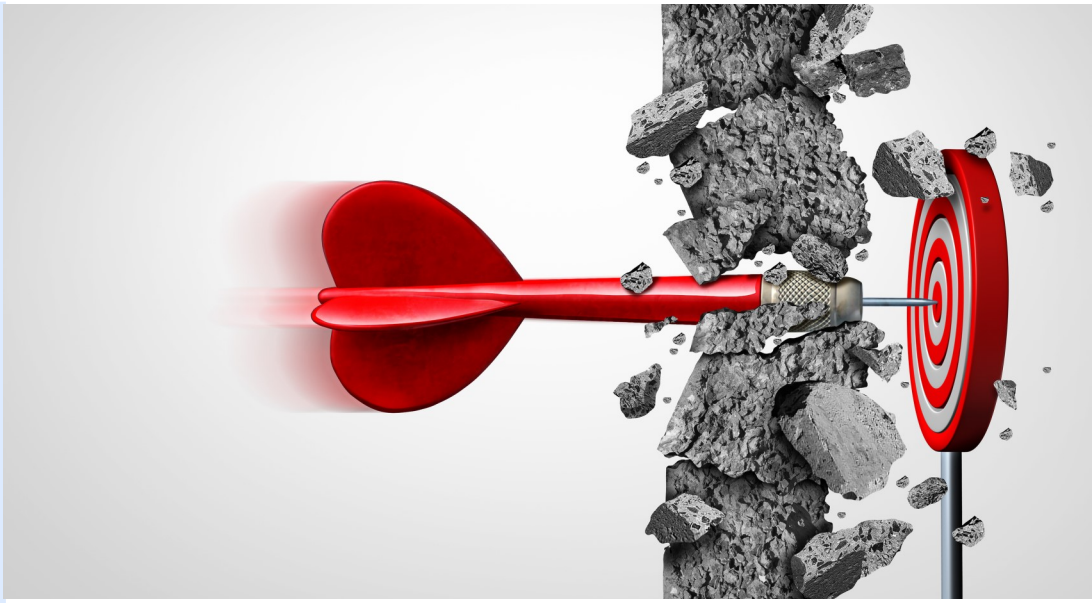
IT Squared Resource, Inc.
1201 Commerce Center Dr.
Franklin, OH 45005

"Your IT and Telecom Advantage!"

August 2018

This monthly publication provided courtesy of Kris Fenton, President of IT Squared Resource, Inc.

Our Philosophy: TO ADD VALUE TO ALL THOSE WE SERVE. To our clients as a trusted advisor and resource delivering exceptional results. To our employees, through continuous growth, opportunity and flexibility. To our partners and community as active contributors and involved supporters.



Top 4 Ways Hackers Will Attack Your Network

And They Are Targeting You RIGHT NOW

Most small and midsize business (SMB) owners exist in a bubble of blissful ignorance. They focus on the day-to-day operations of their organization, driving growth, facilitating hiring and guiding marketing, without a single thought given to the security of the computer networks these processes depend on. After all, they're just the little guy – why would hackers go to the trouble of penetrating their systems for the minuscule amount of data they store?

And eventually, often after years of smooth sailing through calm seas, they get hacked, fork out thousands of dollars to malicious hackers and collapse beneath the weight of their own shortsightedness.

The facts don't lie. According to Verizon's annual Data Breach Investigations Report, a full 71% of cyber-attacks are aimed squarely at SMBs. And while it's unclear exactly how many of these attacks are actually successful, with the sad state of most small businesses' security protocols, it's a safe bet that a good chunk of the attacks make it through.

But why? As Tina Manzer writes for Educational Dealer, "Size becomes less of an issue than the security network … While larger enterprises typically have more data to steal, small businesses have less secure networks." As a result, hackers can hook up automated strikes to lift data from thousands of small businesses at a time – the hit rate is that high.

Today, trusting the security of your company to your son-in-law, who assures you he "knows about computers," isn't enough. It takes constant vigilance, professional attention and, most of all, knowledge. Start here with the four most common ways hackers infiltrate hapless small businesses.

1. PHISHING E-MAILS

An employee receives an e-mail directly from your company's billing company, urging them to fill out some "required" information before their paycheck can be finalized. Included in the very professional-looking e-mail is a link your employee needs to click to complete the process. But when they click the link,

Continued on pg.2

Continued from pg.1

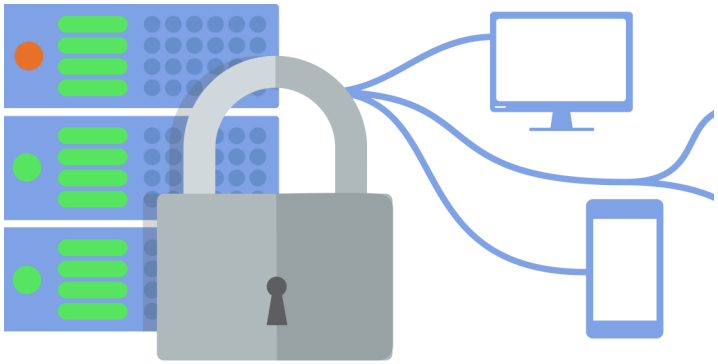
they aren't redirected anywhere. Instead, a host of vicious malware floods their system, spreading to the entirety of your business network within seconds, and locks everyone out of their most precious data. In return, the hackers want thousands of dollars or they'll delete everything.

It's one of the oldest tricks in the hacker toolbox, but today it's easier than ever for an attacker to gather key information and make a phishing e-mail look exactly like every other run-of-the-mill e-mail you receive each day. Train your employees to recognize these sneaky tactics, and put in safeguards in case someone messes up and clicks the malicious link.

2. BAD PASSWORDS
According to Inc.com contributing editor John Brandon, "With a $300 graphics card, a hacker can run 420 billion simple, lowercase, eight-character password combinations a minute." What's more, he says, "80% of cyber-attacks involve weak passwords," yet despite this fact, "55% of people use one password for all logins."

As a manager, you should be bothered by these statistics. There's simply no excuse for using an easy-to-crack password, for you or your team. Instead, it's a good idea to make a password out of four random common words, splicing in a few special characters for good measure.

3. MALWARE
As described above, malware is often delivered through a shady phishing e-mail, but it's not the only way it can wreak havoc on your system. An infected website (such as those you visit when you misspell sites like Facebook.com, a technique called "typosquatting"), a USB drive loaded with viruses or even an application can bring vicious software into your world without you even realizing it. In the past, an antivirus software was all that you needed. These days, it's likely that you need a combination of software systems to combat these threats. These tools are not typically very expensive to put in place, especially considering the security holes they plug in your network.



"...hackers can hook up automated strikes to lift data from thousands of small businesses at a time — the hit rate is that high."

4. SOCIAL ENGINEERING
As fallible as computers may be, they've got nothing on people. Sometimes hackers don't need to touch a keyboard at all to break through your defenses: they can simply masquerade as you to a support team in order to get the team to activate a password reset. It's easier than you think, and requires carefully watching what information you put on the Internet – don't put the answers to your security questions out there for all to see.

We've outlined some of the simplest ways to defend yourself against these shady techniques, but honestly, the best way is to bring on a company that constantly keeps your system updated with the most cutting-edge security and is ready at a moment's notice to protect you in a crisis. Hackers are going to come for you, but if you've done everything you can to prepare, your business will be safe.

FREE Report: 12 Little-Known Facts Every Business Owner Must Know About Data Backup And Disaster Recovery

You will learn:

- 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.
- 7 things you should absolutely demand from any off-site backup service.
- Where many backups fail and give you a false sense of security.
- The No. 1 cause of data loss that businesses don't even think about until their data is erased.

Claim Your FREE Copy Today at
www.it2resource.com/12facts

Shiny New Gadget Of The Month:

An Indoor, No-Hassle Cookout: The Kenyon City Grill

As we draw close to the end of summer, many of us are stowing our grills in preparation for the cooler months. Others never had a grill in the first place, banned by their lease from ever doing any sort of grilling. Regardless of the reason, pretty much everyone bemoans a grill-free existence, even if it's only for a few months.

Enter the Kenyon City Grill, a handy grill for those of us who need to stay inside to cook up a hot dog or hamburger. With some complicated engineering tricks, the grill can cook anything you throw at it with virtually no smoke, far exceeding the requirements of city fire codes and preventing you from getting smoked out of your kitchen. Its $475 price tag may seem a little steep, but consider the convenience of grilling right from your kitchen, all year long – even if you're in an apartment! – and you can quickly see the benefits.

8 Tendencies Of Bad Decision Makers

At one point in my career, after I'd started, grown and sold a couple of businesses, I thought I knew everything there was to know about making good decisions. After all, I was a success! But it took me a few years to realize that, in many respects, I still had a lot to learn about making the best calls. Here are the lessons I learned the hard way back then about the tendencies and motivations of people who are making the worst business decisions of their lives.

BASING DECISIONS ON EGO
If you think you know it all and that your expertise in a narrow field will translate to every other field, you're just flat wrong. Assemble a team of folks whose experience rounds out your own and reap the benefits of multiple perspectives.

RELYING ON THE MOMENTUM EFFECT
There's certainly some truth to the belief that past events can predict future events. The problem with this thinking, though, is that the world is constantly evolving. If you're sticking with the tried-and-true and refusing to look at other options, you're likely to misstep.

BEING LAZY
Entrepreneurs have to be hungry and curious. Make sure you're looking at the whole picture, and at both the negatives and positives of any potential decision.

BEING INDECISIVE
If you're putting off making a choice, you can end up limiting your options down the road. You may be right, you may be wrong, but don't let yourself get cheated out of success.

GOING IT ALONE
You simply can't understand all the options and complexities of a given situation on your own. Sometimes the best results come through compromise with a team you've assembled.

EXECUTING POORLY
Making a decision is only 10% of the process. The other 90% is the actual execution of that decision. If you fail to communicate the reasons for your decision to your staff, neglect to plan or follow up, or simply drop the ball, you're not getting the job done. Make sure you implement your changes in a thoughtful, logical way.

SEEING THE TREES RATHER THAN THE FOREST
Good decisions are made with the big picture in mind. If you're focused on putting out fires or only thinking about next week, you're not going to be able to adequately plan ahead. Leave the short-term decisions to your trusted staff and devote your energy to the long term.

NOT BALANCING YOUR SOURCES
Abraham Lincoln was a great president, but it wasn't just because he was a smart, thoughtful man. He surrounded himself with a cabinet comprised of his most bitter rivals, understanding the power of hearing from people other than "yes" men. Don't fall into the trap of listening to sycophants who tell you only what you want to hear. By seeking out contrary opinions, you'll avoid making decisions based on biased sources.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group. He is also a former small-business columnist for The Wall Street Journal*; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book* The Toilet Paper Entrepreneur. *His newest book,* The Pumpkin Plan, *has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com.*

CYBERSECURITY TIPS FOR TRAVLERS

Before You Go

-Update your mobile software. Your mobile device IS a computer. Keeping the operating system and apps up to date will help defend against malware.
-Back up your information. Back up your contacts, photos, etc. to another device or cloud service.
-Keep it locked. Be sure to lock your device when you are not using it. Use a strong PIN or password to protect unwanted access.

Top Ways To Stay Secure In The Social-Media World

Social media allows millions of people to reconnect and stay up-to-date with family members, friends, acquaintances and even former in-laws. But as social media reshapes the way we communicate with one another, it's important to keep a couple of things in mind to protect yourself and your data.

Remember that there's no "delete" button on the Internet. Even if something seems temporary, a simple screenshot or check through the archives can make it permanent. Even if you keep your social media completely private, relationships change, and what was private yesterday may suddenly become public record. The question you need to ask is whether you'll be comfortable in 10 years with what you're posting today.

In the same vein, if you post in online forums or on message boards, consider using a pseudonym. Never share names of real businesses, clients, friends or family. If a bank manager wouldn't allow a picture of all the money in the vault to be shared on the web, you shouldn't allow a picture containing confidential, financial, legal or other protected documents and items to be shared either. A good social-media policy in the office now can save headaches down the road.

9 Quick Tips To Protect Your Business From Cyber-Attack

Cyber security is more important than ever, but it doesn't have to be complicated.

Just follow these rules and you'll be well ahead of the game:

1. Only use secure networks.
2. Encrypt your data – it's easier than it sounds.
3. Install a strong firewall.
4. Install patches and updates as soon as they become available.
5. Do your research on the most common cyberthreats (you'd better know what phishing is).
6. Develop a company-wide cyber security policy.
7. Make sure your business WiFi router is protected by the WPA2 standard. (Look it up.)
8. Install software that insulates you from malware.
9. Get SSL (Secure Sockets Layer) Certificate Protection, especially if you take payments online.

SmallBizTrends.com, 4/25/2018