The Cyberian Chronicle

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

What's Inside?

December 2017

This monthly publication provided courtesy of Andy Banning, Senior Account Manager of Cyberian Technologies.

cyberian technologies

Cybercriminals Confess: The Top 5 Tricks, Sneaky Schemes And Gimmicks They Use To Hack Your Computer Network

The contemporary world is rife with digital thieves. They're penetrating the complicated data structures of huge credit-monitoring companies like Equifax, scooping up the personal information of millions of people. They're releasing sensitive customer data to the public from discreet businesses like Ashley Madison. They're watching webcam feeds of our celebrities without them knowing; they're locking down the systems of public utilities like the German railway system; they're even managing to steal thousands of gigabytes of information directly from high-profile government entities like the CIA.

They're also targeting small businesses exactly like your own and extorting them for thousands and thousands of dollars.

When running a company, it's vital to have a dedicated security team, equipped with the most up-to-the-minute security technology, on your side to protect you from these malicious cyber threats. But it's not enough to leave it to somebody else. You also need to be informed. Here are five of the most common ways hackers infiltrate your network:

1 Phishing Scams

You receive an e-mail in your work inbox coming directly from a high-ranking employee with whom you've been working on a project. Inside is a link he needs you to click to access some "vital information," but when you click it, it rapidly installs a host of malware on the computer, spreads through the network and locks out everyone in the company.

Phishing scams are the oldest trick in a hacker's book – ever received one of those "Nigerian Prince" scams? – but they're still wildly successful. Not only that, but they're becoming increasingly more sophisticated. As Thomas Peters writes for "Newsweek," "The

Continued on pg.2

Continued from pg.1

best messages look like they're trying to protect the company. One well-meaning system administrator even offered to post a PDF that could deliver malware on an internal server because it was called, 'How to avoid a phishing attack.'" How's that for irony?

2 Social Engineering

Social engineering is a type of "hacking" that uses real, well-intentioned people to carry out its schemes, rather than intricate lines of code.

This is especially effective for gathering sensitive information that can later be used in another type of attack – e-mail passwords used for phishing scams, for example. Maybe your IT guy receives a call from the "secretary" of one of your clients, pretending that they're experiencing problems with your service due to some firewall, a problem that your IT professional is more than happy to help out with. Before you know it, the caller knows the ins and outs of your entire security system, or lack thereof. Social engineers have been known to use phone company customer service departments, Facebook and other services to gather Social Security or credit card numbers, prepare for digital robbery and even change the passwords to your central data network security.

3 Password Hacking

You may think that your passwords are clever and complicated, filled with exclamation points and random numbers, but it's rarely enough. With information gathered carefully from social engineering or a simple check on your employees' social media accounts, hackers can easily use brute-force to figure out that your password is the name of the family dog, followed by your anniversary (for example). That's if they didn't already manage to steal your password through one of the techniques listed above.

> **"When running a company, it's vital to have a dedicated security team, equipped with the most up-to-the-minute security technology, on your side to protect you from these malicious cyber threats."**

4 Fault Injection

Sophisticated hackers can scan your businesses' network or software source code for weak points. Once they're located, they can surgically attempt to crash the system through snippets of code they splice in expressly for that purpose. Different commands can do different things, whether they want to deliver a devastating virus, redirect links on your website to malicious malware or steal and erase vast swathes of information.

5 USB-based Malware

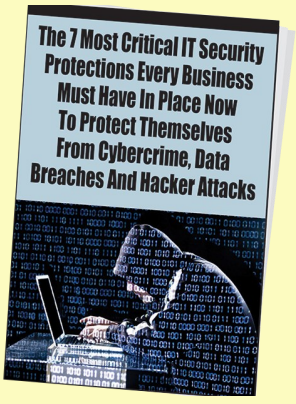
At the last conference you attended, someone probably handed out free branded USB sticks to keep their business top-of-mind. Hackers will sometimes covertly slip a bunch of infected USB sticks into a company's stash. The instant somebody tries to use one, their computer is taken over by ransomware.

So What Can I Do About It?

It's a scary world out there, with virtually everyone left vulnerable to digital attack. Knowing the strategies hackers deploy is half the battle. But, frankly, these techniques are constantly changing; it's impossible to keep up by yourself.

That's why it's so important to utilize only the most up-to-date security solutions when protecting your business. Hackers move fast. You and your security technology need to stay one step ahead.

FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious reputational damage, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Claim Your FREE Copy Today at: http://www.cyberianit.com/7securityprotections/

Attend Cyebrian's LIVE Webinar on Cybersecurity: December 14th, 2017 at 10:30A.M. Est.

12 Ways To Keep Your Business Safe From Cybercrime

Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of small businesses to sell credit cards and client information, and swindle money directly out of your bank account. Some are even funded by their own government to attack small, virtually defenseless businesses.

As a local IT support company, we work day and night to protect our clients from these attacks - and unfortunately we see, on a regular basis, hardworking entrepreneurs being financially devastated by these attackers. We are determined to WARN as many businesses as possible!

Register for the webinar today: https://12waystokeepyourbusinessafefromcybercime.eventbrite.com

5 Ways To Handle Bad News In The Workplace And Move On

Every company has its ups and downs. How your organization deals with those intermittent challenges is just as important as how it celebrates its victories, if not more so. Maybe your quarterly earnings have come in below expectations, or maybe a long-admired senior manager has decided to leave the firm. Maybe you've had to let someone go, or maybe the team isn't reaching its potential. As a business leader, you need to relay the news to your team quickly – in a way that doesn't have any additional repercussions, like hurting the company culture. But how do you do that?

Talk About It

It may sound simple, but it's anything but. Clear and open communication doesn't come naturally to many leaders. So, you have to be intentional about it. If you know something bad is going to happen (or already has), gather your team in a room as soon as possible to talk about the news. Opening up the conversation is the single most important step.

Be Transparent (Don't Sugarcoat The Bad News)

It's no use gathering your team to share news if you're going to hold back information. When times are tough, trust is often the first thing to erode if people feel like they're not being told the whole truth. Ensure that when you gather your team to talk, everything is on the table – no secrets. Bad news is bad news; there's no sense trying to spin it positive. You have to be genuine.

Hear From Everybody

The opinion of a senior vice president should have no more weight than that of your front-desk receptionist. If you want a real team atmosphere, you have to be willing to hear everyone's voice and address any questions or concerns. This will go a long way toward reinforcing that "we're all in this together" feeling and the fact that you're open to differing opinions. Whether or not you can answer every question or address every issue isn't important, but listening to each person is crucial.

Determine A Path Forward

It's not enough to get things out on the table. You have to be able to move forward in a deliberate way. Once everyone has been heard, make a plan for how things are going to proceed. Maybe you develop a way for each team member to contribute to bringing in new business or recruiting top performers. Whether the task is small or large, be sure you make a plan to address any underlying problems that may have caused the issue in the first place. Get buy-in from your team and get to work.

As the founder of Petra Coach, Andy Bailey can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success, and coaching them past the excuses we all use to avoid doing what needs to be done. Andy learned how to build great organizations by building a great business, which he started in college. It then grew into an Inc. 500 multimillion-dollar national company that he successfully sold and exited.

Become A Better Public Speaker With This App

Americans are terrified of public speaking. In fact, in most surveys about our fears, talking in front of a crowd far outranks even our fear of dying. But if you, like millions of others, break out in a cold sweat when you imagine giving a speech, you're in luck. There's an app for that.

Developed during the Disrupt San Francisco Hackathon, Vocalytics is a comprehensive project dedicated to building an AI that will teach you to be a better public speaker. The ultimate goal is to develop a virtual trainer that can give feedback even better than what you'd get from a professional speaking coach.

The app – called Orai – uses machine learning to analyze your body language as you speak, ensuring that every word hits home. When paired with speech analysis project SpeechCoach.ai, you can take concrete steps toward killing it in front of any crowd.
TechCrunch.com 9/17/2017

Cyberian's New Team Members!

Jeff **Kelm**

Jeff performs as a Level 2 and helpdesk engineer for Cyberian. He holds a Bachelors of Science in Information Systems and an Associates in Electronics. Prior to Cyberian, Jeff spent 20 years in the United States Air Force with multiple roles. He spent 16 of those years in Copper and Fiber Optic splicing, radio, microwave and satellite antenna installation/maintenance and 12 years in management roles. Jeff has also received his CHTS-PW (Certified Healthcare Practice Workflow & Information Management Redesign), received his PMC (Professional Manager Certification), from the Air Force, and is also a BICSI Level 2 installer for Copper and Fiber Optic splicing and backbone infrastructure.

John Roberds

John is one of our tier 3 helpdesk Engineers. He has an Associates in Electrical Engineering Technology from Purdue University and has specific skills in Cisco networking, VMware, VDI, Windows Server, and Veeam. John was previously employed with the Federal Judiciary of the United States, where he performed as a Network Systems Engineer for 15 years.

William Johnson

William is finishing up his Senior year at Indianapolis University Purdue University Indianapolis with a Bachelors in Computer and Information Technology with a concentration in Networking Systems. William's primary responsibility with Cyberian is performing as a Helpdesk Technician assisting our clients with various needs. Prior to Cyberian, William was employed with Bowen Engineering for a year and a half. This is where he gained the majority of his experience with helpdesk support. Before Bowen, William had two jobs in computer repair shops, where he received the valuable experience with hardware and software repairs on laptops and desktops.

Top Tech Accessories To Make Your Life Easier

The best gadgets help us navigate our lives with ease, making particular processes that much more hassle-free. With technology, it's often the little things that make all the difference in the world. Take AUKEY's car phone mount, for instance. At only $7.99 on Amazon, there's no reason you should be fumbling with your iPhone while you're using Google Maps on a road trip. The clip attaches directly to any air vent, putting your phone front and center for easy viewing and reducing the need for dangerous fiddling.

Or, pair an Amazon Echo with the Tp-Link Smart Plug Mini ($29.99), which allows you to activate all kinds of devices with your voice or your phone. It's the perfect first step toward a smarter home and a world of convenience.

If you've got a phone that's always dying, hook it up to an Anker battery case, which can extend the battery life of most phones by as much as 120%.

For more small-scale tech solutions, check out Business Insider's list of "50 must-have tech accessories under $50."
BusinessInsider.com 9/28/2017