ISSUE 9-1

BITS & BYTES

INSIDER TIPS ON HOW TO USE TECHNOLOGY TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY

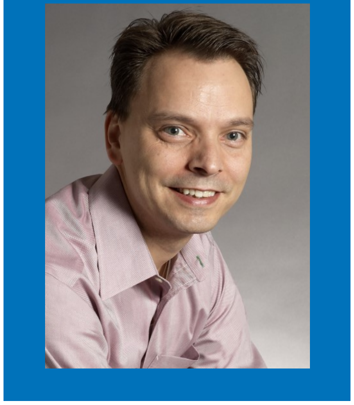
IN THIS ISSUE

January 2018

"TAG specializes in providing management level responsibility for all the technology in your business. This includes support for your network and working with other hardware & software vendors who's technology you use.

We do this with friendly, proactive & responsive service!

Joe Stoll, President
Technical Action Group (TAG)



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 cyberthreats.

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 they need 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 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 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 "admin assistant" 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.

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 adigital 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.

Shiny New Gadget Of The Month:

E-mail Signature Rescue

The business world runs on e-mail. According to LifeWire, around 269 billion e-mails are sent around the world each and every day. But for every e-mail sent, millions go unread, and those that do are often found wanting. How, in the midst of all that noise, can you possibly get your own work e-mails to stand out?

Enter E-mail Signature Rescue (emailsignaturerescue.com), a business dedicated to creating custom, professional e-mail signature templates for all kinds of companies and teams. Using their proprietary software, it's easy to build a robust and beautiful HTML e-mail signature template that will make your e-mails pop. Signatures may seem small, but they can go a long way toward convincing a recipient that you mean business.

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.

Drop These 4 Habits For a Successful 2018

Today, the business world is more rapid, complex, and volatile than ever before in history, a trend that shows no signs of slowing down. With that in mind, it's vital that entrepreneurs tighten up their business practices now, not later.

Here are four bad habits to kick in order to shed your company's sluggishness and step fully into the modern marketplace:

1. Procrastinating training investment: Investing in comprehensive training resources, which expands the skills of both you and your employees, can ensure you stay competitive in the midst of constant change.

2. Amassing knowledge without applying it: With millions of well-meaning advice articles plastered across the Internet, it's easier than ever to learn new principles. But you can't stop there. Actively implement the knowledge you gain, instead of keeping it locked away in your mind.

3. Expecting ideas to come from the top down: Today's savvy business owner doesn't solely channel those at the top of the organization chart. Instead, they welcome ideas from all levels of the company.

4. Busywork: Too many leaders get caught up in output metrics instead of outcomes. Get the numbers out of the way and watch your employees shine. *Inc.com 11/16/2017*

Apps That Make Our Lives Easier, All Under $10

With new apps flooding the market every day, it can be difficult to pick out the ones that will assist you instead of just inspiring buyer's remorse. But there are dozens of apps that, despite their miniscule price tag, can have a small but lasting impact on your day-to-day.

Take Dark Sky ($4) for example. An up-to-the-minute accurate forecasting app that will break down weather information for exactly where you are at any given moment, down to when the expected rain or snowstorm will start and stop.

You can also check out Notability ($9.99), which Business Insider calls "one of the best things to ever happen to note-taking." The app allows you to mark up PDFs and photos, take voice recordings, and a number of other functions, with everything stored in the cloud.

People who have trouble keeping and remembering more than one password might appreciate 1Password (Free), a dedicated place to guard all your passwords behind one difficult-to-hack password. *BusinessInsider.com 10/26/2017*

Become A Better Public Speaker With This App Most people 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*

Are Your Kids Careless With Online Passwords? With corporations taking hits left and right from cybercriminals, security on the Internet has become more important than ever. Still, even as many of us step up the security of our online presence, stragglers who believe they're immune to such attacks abound.

Based on a recent survey from Statista, young people are more careless with passwords. Thirty-four percent of people aged 18 to 34 years use the same password for "most online logins," compared to only 20% of the 35 to 54 demographic, and only 13% for those older than 55. In addition, a whopping 10% of 18- to 34-year-olds use the same password for all their online keys.

It goes without saying that this is bad practice. It can be all too easy to hack into a single, less secure account, but if different passwords are used for separate logins, it becomes much more difficult to access more important files in, say, a Gmail account or bank login. Not so if the passwords are identical. *BusinessInsider.com*