May 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

BITS & BYTES

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

5 Ways Your Employees Will Invite Hackers Into Your Network

Whether they're criminals or heroes, hackers in the movies are always portrayed as a glamorous group. When it comes down to the wire, these are the individuals who crack into the ominous megacorporation or hostile foreign government database, hitting the right key just in the nick of time. They either save the day or bring down regimes, empty the digital vault of the Federal Reserve or disable all the power plants in the country. It's always a genius up against an impenetrable fortress of digital security, but no matter what, they always come out on top.

In real life, it's rarely that difficult. Sure, if you look at the news, you might believe hackers are close to their Hollywood counterparts, stealing data from the NSA and nabbing millions of customer records from Equifax. But the majority of hacks aren't against the big dogs; they're against small to mid-sized businesses. And usually, this doesn't involve actually hacking into anything. A lot of the time – approximately 60% according to the Harvard Business Review – an unwitting employee accidentally leaves the digital front door open.

The biggest threats to your company aren't teams of roaming hackers; they're your employees. Here's why.

1 They'll slip up because they don't know any better.

With the proliferation of technology has come an exponential rise in digital threats of such variety and complexity that it'd be impossible for the average person to keep track of it all. Each of your employees' lives are a labyrinth of passwords, interconnected online accounts and precious data. If their vigilance slacks at any point, it not only leaves them vulnerable, but it leaves your company vulnerable as well. For this reason, most cyberattacks come down to a lack of cyber security education.

2 They'll let you get hacked on purpose.

It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data to malicious groups. Whether it's info vital for your competitive advantage, passwords they can sell to hacker networks to make a quick buck or sensitive data they can make public simply to spite your organization, it's difficult to protect against a double agent.

3 They'll trust the wrong person.

For many hacks, little code is needed whatsoever. Instead, hackers are notorious for posing as a trusted member of your own team. And if you believe that you'd be able to spot an impostor from a mile away, you may want to think again. Not only is it easier than ever to crack individual users' e-mail passwords and login credentials, and personal info is now littered throughout social media. A simple visit to Facebook can give a hacker all they need to know to "social hack" their way into the heart of your business.

> "It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data… [b]ut there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people."

4 They'll miss red flags while surfing the web.

Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

5 They're terrible at passwords.

According to Entreprenuer.com, "3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more." Even more of those passwords are simply weak, inviting easy access for unsavory elements. Many people brush off the importance of strong passwords, but the risks posed by the password "123456" or "password" cannot be overstated.

When it comes to defending your precious assets against digital threats, it can seem impossible to protect yourself at every turn. But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people. Through a comprehensive security training program, including specific examples of methods hackers use – particularly phishing – you can drastically minimize the risk of an employee accidentally opening up a malicious e-mail or posting sensitive info. When you make a concerted effort to make the entire organization vigilant against cyber-attacks, you're much less likely to be targeted.

Copyright 2008 by Randy Glasbergen.
www.glasbergen.com

"Instead of waiting for someone to steal my identity, I'm going to auction it on eBay!"

Cash In On Your Million-Dollar Idea

So, you came up with a brilliant idea. A million-dollar idea, even! But right now, that's all it is. The question is, how do you turn that big concept into cold, hard cash?

1. Write it down. How many light-bulb moments do you have at 2:00 a.m. and then forget come 9? Or, worried that your idea will be stolen, you keep it to yourself, promising to chase it down when you finally get the time. If you actually write down every money-making scheme you think up, one of them is bound to be the real deal eventually.

2. Once you settle on the idea you want to pursue, write a pros-and-cons list. What could make your idea truly successful? What could make it a total bust? Once you identify the cons – a too-high initial production cost or a newcomer in a competitive industry – you can start your search for solutions.

3. Determine your audience. Who do you think will buy your product or service? Run business surveys to determine whether there's a market for what you want to sell.

4. Figure out what problem you're solving. Uber eliminated the inconvenience of hailing a taxi and the difficulty of pre-ordering a ride, all for an affordable rate. Apple lowered the cost of technology and made it user-friendly at a time when computers were designed for engineers and tech professionals. If you solve a real problem that exists in the market, consumers won't be able to live without your product.

5. Find a business partner. Although you may want to keep your idea to yourself, remember that it takes two flints to make a fire. How many successful start-ups do you know that were founded by a single person?

6. Start to think about money. If you don't already have some rainy-day funds to dive into, consider crowdfunding, borrowing from friends, credit cards or loans. Know the risks you're taking before moving forward.

7. Create a financial model. If you want to attract investors, a financial model that forecasts the fiscal performance of your business will show them your expected profitability and their return on investment. This makes you a more reliable bet.

8. Develop your prototype or beta test. This will allow you to see if your idea will actually work in the real world.

9. Prepare to be flexible and roll with the punches. Odds are, your initial idea won't be the same as your final product, and that's okay.

10. Keep on the sunny side. There are going to be truckloads of people who try to tear you and your idea down on your road to success. Stick to your guns – it's your baby and your investment of time and money, so make sure you believe in it.

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, a consulting firm that ignites explosive growth in companies that have plateaued; 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.*

5 Tips To Avoid Outrageous Cell Phone Charges When You Travel

If you're like most business owners, you need to stay tapped into your business and connected to your family from wherever you are, and you don't want to spend a fortune doing it. If you've come home to a whopping cell phone bill while you've been out of town, these tips to can help you minimize the pain on future trips abroad.

1.   Alert Your Circle

It's important to let anyone who needs to get in touch with you know that you will be out of town. Explain that texting or calling using conventional methods will incur extra charges for you. Also be sure to advise them when you will return so they can plan accordingly.

2.   Setup Alternative Communication Methods

Setup an application that leverages a data plan or Wi-Fi connection, such as Skype. Let your contact list know how to contact you via these apps, instead of using regular text messages or phone calls. Keep in mind that these apps will only work when you are in Wi-Fi range or if you have a data plan setup, so plan accordingly.

You may also choose to purchase a separate texting plan for the area where you'll be traveling. Make sure you check the prices before you leave, as some plans are atrociously expensive.

3.   Use Wi-Fi for Email Whenever Possible

Be sure you are using a Wi-Fi connection whenever possible to check your email throughout your trip. Of course, not just any connection will do. You'll want to make sure your Wi-Fi connection is reputable. .

Also, be selective about downloading attachments. If possible, wait until you are back in your hotel or office, and download the attachments while connected to Wi-Fi .

If you'll be away for an extended period of time, you might want to look into buying a data plan through your internet provider for the location where you're traveling.

4.   Phone Calls

If you don't like the idea of using alternative services, like Skype or Viber for phone calls, see if you can get a voice plan through your provider for the country where you're traveling This is most advantageous if you'll be away for an extended period.

Phone carriers like Roger's offer 'Roam Like Home" for as low as 7 bucks a day in the US, and 12 bucks a day in many international destinations) which is an economical option if you're out of town for a short duration. You might also investigate the possibility of purchasing a phone in the country where you're traveling since their local phone plans may be cheaper than the one through your regular provider.

5.   Internet and Third Party Applications

Be very careful about how often and when you surf the internet or use apps such as Google Maps, Trip Advisor, Weather, iTunes, etc. Whenever possible, use these apps while on Wi-Fi to minimize cellular data plan charges which are always much more expensive when you are outside of Canada, and can eat into your plan pretty quickly.