COMPUTER WORX
INFORMATION TECHNOLOGY

Digital Times

"Practical Advice To Make Your Business Run Faster; Easier And More Profitably"

"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!"
- Jay Burgess, President
Computer Worx

MARCH 2018
THE COLORADO FRONT RANGE

Inside This Issue…

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

continued on pg2

continued from pg1

cyber-attacks 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… but 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.

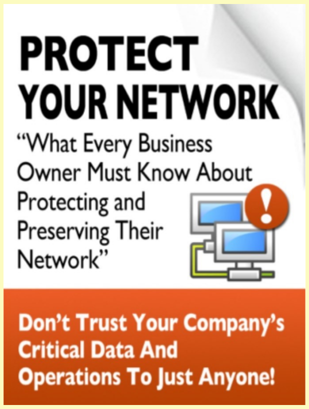
Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

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.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems



PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"

Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This report will outline in plain nontechnical English common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Claim Your FREE Copy Today at www.ComputerWorxIT.com/Protect

Time Out Trivia: Where and when was the first St. Patrick's Day parade?

Shiny New Gadget Of The Month

FIXD

When was the last time you turned on your car, pulled out of the driveway and suddenly noticed the engine light pop up on your dashboard? You probably just ignored it and drove to your destination. Maybe the next day you spent some time trying to get to the bottom of the issue, only to come up short. Everything seems fine, so what's going on?

A new device called FIXD aims to figure that out. After plugging in the $59, palm-sized widget into your car's onboard diagnostics port – the same one mechanics use to find potential issues – it can communicate with a free app to tell you precisely what's wrong with your vehicle. You can determine why your engine light is on, how serious the problem is, and whether it requires emergency repairs, all without risking being ripped off by shady mechanics. If necessary, the device can actually turn off your engine light right from the app, making it a nuisance of the past.

Team Meeting with Nate Hutton

By B. Stanton

B: Nate, as a Colorado native, what three words describe your Colorado? N: Clean, Active, and Hi-Tech. B: Have you ever had the desire to live somewhere else? N: I've lived in New York and Arizona. B: Where in New York N: NYC, by Madison Square- I lived there for a month and realized it wasn't for me. B: Where in Arizona? N: In, Phoenix I was at my friend's house, out on the patio, after midnight and it was still 103 degrees- that was enough. B: Where is your favorite place to be? N: My favorite, Iceland. It's kind of like a Utopia. The people are friendly, active, it's everything you can do outdoors. I love the Viking culture.

B: Speaking of keeping active, how long have you been competing in fitness competitions? N: A long time, I don't compete anymore…, but for about 10 years. I quit in my 30's. Life happened. Married, Kid, Family – a new chapter. B: How does your workout routine mirror your work ethic? N: You're not being paid to work out. It's a level of personal maturity, you build yourself up while not getting paid, then you get paid and with that comes satisfaction. B: When did you realize that IT was what you wanted to pursue? N: That's a tough question. I rebuilt my first computer when I was 9, All my life really, I just had to go through the schooling and training. I was rebuilding computers for people when I was 14 or 15. B: Do you share any information about yourself online? N: Not really, there is so much out there with people doing it full-time. It would really be just a speck of dust in a pile of dust.

B: What technology-related websites or blogs do you follow? N: I follow a couple on a regular basis- theverge.com, Boy Genius Report BGR.com, and cnet.com B: How do you keep your technology skills current? N: Being obsessed with technology I am interested in it all the time. It keeps me current, it is also my hobby.

B: So, Beck, Clapton or Page? N: Not Beck, I am going to have to go with Clapton. I'm a huge guitar enthusiast – and he's done some pretty, awesome stuff. B: What was the 1st song you learned to play? N: Oh Boy (contemplating)… Metallica's *Nothing Else Matters*. B: What have the last few years taught you? N: You'll never know everything. Right when you think you have it figured out there is going to be a curveball.

B: Can you tell me about a recent project or process that you made better, faster, smarter or more efficient? N: A client recently switched to an internet provider that usually configures the switches, but not this time. I have experience with configuring switches – just not Cisco, so it was good to expand my knowledge and know how they work. B: What are your favorite and least favorite technology products, and why? N: My Favorite tech is the iPhone. It changed the way we operate as an entire world. My least favorite, … not a lot I won't try. AI (Artificial Intelligence) scammer bots, that's the best way I can put it.

B: Being an engineer who deals face to face with clients you often take on the role of a teacher. What are the essentials when sharing a new technology? Patience is Number 1, Number 2 is humanity. You must understand, that they don't know what you know – you never want to be condescending. B: What are two or three major trends affecting the IT industry and how do you see them affecting the profession? N: Number one is security. It is constantly becoming more sophisticated, causing us to stay on top of it. Number two: Cloud Service. There is almost no reason not to have it, unless someone feels it's untrustworthy… but Cloud Services are for sure.

B: What was the last song you sang in your car? N: Hang on, I will tell you (reaching for his iPhone) Lincoln Park- *Invisible*

B: And finally, how do you define success? N: I think if you are happy, you are successful!

Tidbits

7 Things Mentally Strong Leaders Never Do

Leaders need to stay mentally sharp to effectively lead their teams. Here are seven things that truly strong leaders never, ever do.

1.They don't mask their insecurities, but instead maintain their humility and acknowledge their mistakes and weaknesses.

2. They don't go overboard with their emotions. Instead of suppressing their feelings, real leaders stay aware of how their emotions influence their behavior.

3. They accept criticism with open arms. Instead of protecting a fragile ego, mentally strong leaders take unfavorable feedback and use it to improve their processes.

4. They take responsibility for their actions. When a good CEO messes up, they apologize with sincerity and accept the consequences of their behavior.

5. They don't mistake kindness for weakness. Offering extended bereavement leave isn't letting your employees take advantage of you – it's a common courtesy.

6. They don't confuse confidence with arrogance. Though they're sure of themselves, a good leader recognizes the necessity and competence of their team. They don't put themselves over others.

7. They don't fear other people's success. When someone else is doing great things, they know that it doesn't diminish their own accomplishments.
Inc.com 12/12/2017

The "Not Me!" Problem… And Why This Is Almost Guaranteed To Happen To You

Security this, password that – now they want a password with 14 characters with two symbols? And I have to change it every three months? As difficult as it is to remember 24 different passwords, four PIN numbers and a slew of new cyber security processes, we still manage to instantly recall most of the tangible things in our lives. The code for the company door and alarm system, the passcode to our phones, the garage code, the other garage code – you get the idea. But these numbers are based upon a time when the most "real" threat seemed to be someone busting in our door and threatening our families in the middle of the night. In 2018, those kinds of physical threats are far less statistically prevalent than cybercrime. In fact, data breaches and identity theft are occurring at three times the rate that home burglaries occur in the U.S. according to a 2016 study by the University of Kentucky.

Don't succumb to the "Not me!" approach to the shift in crime. Understand that it can happen to you, and approach all aspects of physical and electronic security with the attention they deserve.

About Town

Your Monthly Entertainment Options

Friday March 9
Shovels & Rope
Boulder Theater

Leftover Salmon Festival
Stanley Hotel

Saturday March 10
The Fragile Bee
Loveland Museum

Sunday March 11
k.d. lang
Paramount Theater

Wednesday March 14
Glen Hansard
Boulder Theater

Friday March 16
Dead Sea Scrolls
Denver Museum of Nature & Science

Saturday March 17
Sam Bush
Boulder Theater

Tuesday March 20
The Bad Plus
DazzleJazz Restaurant & Lounge

Thursday March 22
Arturo Sandoval
Lincoln Center

Friday March 23
Buddy Guy
Paramount Theater

Thursday March 29
Michael Schenker Fest
Cervantes Masterpiece Ballroom

Friday March 30
Medeski Scofield Martin & Wood
Ogden Theater

Trivia Answer from p.2: Boston, 1737