TECHNOLOGY TIMES

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

What's New

Rick recently spoke at the ND Rural Water Users Association about Cyber Security and securing SCADA Systems last month.

Previously he has spoken to the North East Dental Association about Security Threats.

If your organization is interested in having Rick speak about Cyber Security or other IT related topics contact us today—info@imsnetworking.com or call 701-364-2718.

March 2018

This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

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;

*Want to Lock-in your IT Costs for the Next **THREE** Years? Sign up for IMS Total Care Services **TODAY**!*

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 cyber-attacks come down to a lack of cyber security education.

> **"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."**

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.

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.

Want information on cyber security training for your employees? Contact us today — info@imsnetworking.com or call us at 701-364-2718.

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.

You Have Four Months To Switch Your Website To HTTPS

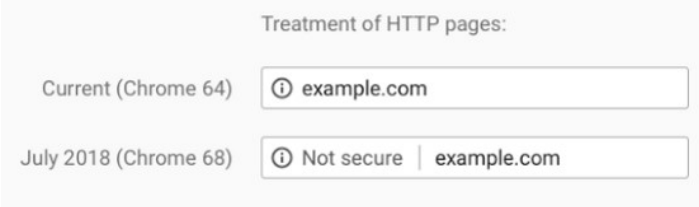
As far as Google is concerned, unencrypted HTTP web connections should be nearing the end of the road.

In 2014 at the I/O conference, it declared "HTTPS everywhere" as a security priority for all web traffic, followed in 2015 by the decision to downrank plain HTTP URLs in search results in favor of ones using HTTPS (where the latter was available).

A year ago, it started labelling sites offering logins or collecting credit cards without HTTPS as 'not secure'.

In a symbolic moment, it has now confirmed that with the release of Chrome 68 in July, this label will be applied to *all* websites not using HTTPS.

It's a small change that streamlines the slightly confusing way Chrome denotes the presence or absence of HTTPS in address bars. From July, the ambiguous grey 'i' icon used to tag many non-HTTPS sites today will disappear, replaced by a simpler 'not secure'. This will look like:



Other browsers (Firefox, Edge, Opera) rely on green or grey padlock symbols to denote HTTPS sites, dropping back to more than one type of grey icon for non-secure HTTP.

But Google's Chrome is the only one to use words and not simply symbols and colors to denote the use of HTTPS. Explains Google:

Chrome's new interface will help users understand that all HTTP sites are not secure, and continue to move the web towards a secure HTTPS web by default.

Getting there?

A look at Google's figures suggests this strategy of coaxing website owners and users to see HTTPS as important is working, with 68% of Chrome traffic on Android and Windows connecting to HTTPS sites. Eighty-one of the top 100 web destinations use it by default.

Some surprisingly big sites such as the BBC apply it inconsistently, using HTTPS for its homepages but dropping back to HTTP for individual content pages (compared to, say the New York Times, which uses HTTPS for everything).

But as more and more sites adopt HTTPS, history suggests getting the last few percent of holdouts to sign up might take a while.

Google's other problem is the old adage about being careful what you wish for: criminals have been seen to exploit HTTPS to gain the trust of users.

No matter how worthy Google's dream of HTTPS everywhere, there's still a lot of work ahead.

Bits & Bytes

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.

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

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.