INTEGRATION
TECHNOLOGY TIMES

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

ISSUE 5 ■ VOLUME 10
■ MAY 2019

What's New

This monthly newsletter is provided courtesy of
Kevin Bowling, CEO of Integration.

"As a business owner, I know 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!"

3 Ways Your Employees Will Invite Hackers Into Your Network

… And What You Must Do To Prevent It TODAY

No matter how professional they are, members of your team – yourself included – are going to make mistakes. It's true of every organization on earth. They'll spill scalding coffee into the company copier. They'll work overtime until the office is empty, then head home without thinking to arm the security system. They'll neglect key accounts, muck up workflows and waste hours developing convoluted solutions to simple problems. And, worst of all, they may unknowingly bumble into the cyber-attack that forces your business to go belly-up for good.

In the majority of cases, that will be by design. There's a saying in the cyber security industry, coined by renowned cryptographer Bruce Schneier: "Only amateurs attack machines; professionals target people." When it comes to repeating the same process safely and autonomously, machines are less fallible than the average person sitting at a desk. Savvy hackers looking to boost funds from unsuspecting small businesses know this. So instead of developing a complex program that dances around the security measures baked into sophisticated modern technology, they target the hapless folks on the other side of the screen. The strategy works disturbingly well. According to IBM's 2018 X-Force Threat Intelligence Index, more than two-thirds of company records compromised in 2017 were due to what they call "inadvertent insiders" – employees who left the front door wide-open for the bad guys without even realizing it. Negligence, lack of awareness and sheer bad luck put the best-laid plans to shame on both sides.

But how does it happen? There are three primary causes of employee-related breaches, each of them contributing to a sizable portion of hacks across the country.

1. Social Engineering

Phishing remains one of the most prominent strategies deployed by hackers to lift data from small and midsize businesses.

……Continued page 2

… Continued from page 1

The majority of these attacks stem from an employee clicking on a suspicious link that is embedded in a dubious or absolutely convincing e-mail. To lure your team into the trap, cybercriminals often use data gathered from cursory investigations of your organization from the Internet or social media. Maybe they pose as a security expert contracting with your company or a member of a customer support team behind one of your employees' personal devices. Whatever mask they wear, it doesn't take much to convince an uninformed individual to click on anything at all, resulting in a high success rate for phishing attacks.

2.Circumvented Or Incorrectly Implemented Security Measures

Even if you do everything you can to protect your business from digital attack, your team may just dodge those measures anyway. According to a report by cyber security firm Dtex Systems, around 95% of companies have employees who will attempt to override previously implemented security processes. And that's if the security measures are configured, patched and installed properly in the first place. The IBM X-Force report lists "misconfigured cloud servers and networked backup incidents" among the chief concerns of last year.

3. Insiders With Malicious Intent

Hell hath no fury like an employee scorned. A strikingly large number of breaches come not from error at all, but from insidious tactics by disgruntled employees or undercover criminals looking to make a quick buck. It's not quite a "you can't trust anyone" scenario, but there are definitely folks out there who would sell your business right out from under your nose.

With each of these in mind, it's vital that you incorporate extensive employee training and vetting protocols to maximize their cyber security know-how. In addition, you need to implement safe practices that reduce the room for human error, alert employees when something is amiss and protect them from the worst.

We can help. It's difficult to overhaul your cyber security, especially on the people side, without a round-the-clock team dedicated to pinpointing the weaknesses in your organization and working to patch them up. In 2019, human error is poised to take an even more central role on the stage of digital crime. Don't leave it up to chance. Partner with an organization that has extensive expertise in training employees on security basics and bolstering your defenses, and head into Q2-Q3 knowing your most precious assets aren't up to the whims of an unlucky employee.

> **"Negligence, lack of awareness and sheer bad luck put the best-laid plans to shame on both sides."**

Quotes and Jokes

“Effectiveness comes from those qualitative things that give you the ability to network, communicate, and lead people toward an outcome they can't see.”

Lynn Good

“Collaboration is important not just because it's a better way to learn. The spirit of collaboration is penetrating every institution and all of our lives. So learning to collaborate is part of equipping yourself for effectiveness, problem solving, innovation and life-long learning in an ever-changing networked economy.”

Don Tapscott

“Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love of what you are doing or learning to do.”

Pele

“Honest communication is built on truth and integrity and upon respect of the one for the other.”

Benjamin E. Mays

“The most important thing in communication is hearing what isn't said.”

Peter Drucker

4 Steps To Protect Your Business After The Marriott Data Breach

Last November, Marriott announced some bad news: the data of up to 500 million customers may have been compromised in an attack. If you travel regularly for business and are a customer of the Marriott chain –including Westin, Sheraton, the Luxury Collection, Four Points, W Hotels, St. Regis, Aloft, Element, Tribute Portfolio and Design Hotels – there are some things you need to do.

First, change your passcodes. This should include your potentially compromised account and any accounts that, for some reason, still use the same login or passcode in 2019. Then, start keeping a close eye on your credit card and bank accounts. You may even want to consider freezing your credit. Finally, be very careful about opening e-mails. Cybercriminals love piggybacking on actual customer contacts from big corporations to send out phishing

e-mails. *SmallBusinessTrends.com, 12/13/2018*

Scanning Documents Has Never Been Easier — Here’s How

Apple’s iOS 11 app is full of exciting new tricks, but the most useful one is a little buried and definitely a lot less glamorous than most: the document scanner inside the Notes app. You no longer need to use a third-party app to upload your documents; you can do it inside Apple’s excellent internal solution.

Just open up Notes, hit the “+” symbol above the keyboard, and tap “Scan Document.” Then all you need to do is select your settings, point it at whatever document you’re trying to digitize and it’ll do the rest. It’ll optimize the picture as a scan and make the document as readable as possible.

TheVerge.com, 8/26/2018

Computer Service

- Pro-Active Customer Care
- Onsite Computer Service/Support
- Network Management/Support
- Network & Server Installations
- Network Security & Firewalls
- Cloud Solutions & Hosted Email
- Secure Remote Access / VPNs

Healthcare Services Provided

- Medical, Dental, Radiology
- Software & Hardware Integration
- Security Solutions

Backup & Disaster Recovery

- Business Continuity
- Secure & Compliant Offsite Backup
- HiTech BDR

Specialize in DFAR planning

Email, Web & Archiving

- Spam Filtering
- Email Hosting
- Email Encryption & Archiving
- Website Hosting
- Customer Hosting Server

VOIP (Hosted)

Ask us about—Managed Services

How would you like to pay a flat rate and have us take 100% responsibility?

How would you like new equipment, service and support for a flat rate and refresh every 3 years?

Integration

Po Box 5526
Decatur, AL 35601
Phone: 256.536.5805

How would you like the security of knowing that your data is safe and protected?

How would you like a VOIP phone system that is cost effective, saves you money, and you can take it home or vacation and work as in the office?