

Technology Today

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"
Since 1984

Back To School Adventures

I just got back from my first week in Boston attending the Goldman Sachs Small Businesses program.



Along with business owners from all over the country, I learned from experts about financials, marketing, business growth and leadership.

My learning and work will continue throughout the next few months and I am so thankful to be able to participate in the amazing program!

October 2017



This monthly publication provided courtesy of Ryan Haislar, Vice President of Computerease.

"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!"

Equifax Employees Share Fake Phishing Website With Potential Victims Of Data Breach

Within the past few months there was a data breach of Equifax's computer network that caused 143 million people to have their personal information including name, date of birth, social security number and even driver license numbers to be leaked.

Instead of contacting each victim directly, Equifax has set up a website www.equifaxsecurity2017.com for each potential victim to enter their personal information and verify if their information was in fact compromised.

Meanwhile, a software engineer, Nick Sweeting, set up a fake phishing website www.securityequifax2017.com in order to increase awareness of a security threat present in the Equifax response to its initial data breach.

A phishing website is set up to look EXACTLY like an authentic website, with the same format and content and also forms to enter your personal data, usernames and passwords. The URL of a phishing website is deceptively similar to the authentic website in order to easily trick people into thinking they are visiting the real website. However, a phishing website is created and managed by hackers who are trying to trick an individual into unknowingly divulging their personal data!

The fake website www.securityequifax2017.com set up by Sweeting did not collect any personal information. Instead, a banner at the top of the site read "Cybersecurity Incident & Important Information Which Is Totally Fake, Why Did Equifax Use A Domain That's So Easily Impersonated By Phishing Sites?"

How easy would it be for a person to type the incorrect URL?

www.equifaxsecurity2017.com

www.securityequifax2017.com

In fact, over the course of a few weeks, the Equifax customer service team directed people to the FAKE WEBSITE in a series of tweets that were responding to consumer's requests for information about <next page>



the security incident.

The tweets have since been deleted and Sweeting's fake website has also been taken down. Equifax has also issued an apology for the confusion but the company is not sure how many people were directed to the incorrect website.

Equifax has issued a warning stating "Consumers should be aware of fake websites purporting to be operated by Equifax. Our dedicated website for consumers to learn more about the incident and sign up for free credit monitoring is <https://www.equifaxsecurity2017.com>, and our company homepage is Equifax.com. Please be cautious of visiting other website claiming to be operated by Equifax that do not originate from these two pages." Will this simple warning be enough to protect consumers? Only time will tell.

What is the responsibility of a business to safeguard their client's data?

A client is paying you for a product or to provide a service and they trust that you are taking measures to secure their data. As a business owner or administrator there are cyberattackers and hackers that would love nothing more than to have you or one of your employees make a small and innocent mistake, or for you to NOT take proactive security measures to protect your client's data.

If there was a data breach of your systems, what would your response be?

What would the impact of a security incident be for your business?

Take action NOW to protect your business, your client's sensitive information and plan for the worst. Our FREE webinar on November 8th at 10:33am will cover all the information that you need to not end up like Equifax.

Get all of the details and register for the webinar at www.computer-service.com/free-cybersecurity-webinar or call us today at (314) 432-1661 (MO) or (618) 346-8324 (IL).

What does "phishing" mean?



A phishing scam uses fake emails and websites as lures to trick people into handing over sensitive information. Some of the earliest hackers were known as "phreaks" and the term "phishing" was used to link these scams with the hackers who developed them. The first time the term "phishing" was used was as early as January 2, 1996.

What is "spear phishing"?

Spear phishing refers to a targeted email that is personalized for the recipient that is from an apparent trusted source, but instead it leads the unknowing person to a fake website containing malware.

Scary Facts About "Phishing"

- 91% of cyberattacks start with a phishing email
- 400,000 new phishing websites per month (*Webroot Quarterly Threat Trends Report*)
- Spear phishing has netted 2.3 billion since 2013 (*FBI*)

Free Cybersecurity Webinar - November 8th 10:33am

"7 Critical IT Security Protections EVERY Business Must Have In Place NOW To Avoid Cyber Attacks, Data Breach Lawsuits, Bank Fraud and Compliance Penalties"

During This Webinar You'll Discover:

- The #1 critical security threat to your business that most IT departments never address - and that your organization is neglecting
- Why antivirus and firewalls provide only base-level protection, and how cybercriminals easily sneak around those to hack your business
- How to avoid having to pay a ransom to hackers - even if they lock your data and corrupt your files



Register today at www.computer-service.com/free-cybersecurity-webinar

*Get More Free Tips, Tools and Services At: www.computer-service.com
(314) 432-1661 (MO) or (618) 346-8324 (IL)*

Client of 15 Years Wins Referral Contest!

Thanks to everyone who participated in the Summer Baseball Referral Contest!

Even though this referral contest has ended, you can still earn some awesome rewards for referrals.

Check out the details on our website: <http://www.computer-service.com/about-us/referral-program/>

Comprehensive IT Support Company That Understands Business

My medical practice and billing company have used Computerease since 2002 for IT support. During this time we have done everything from move locations, implement new practice management, EMR software, and PACS, comply with HIPAA and HITECH, merge companies and much more.

Computerease has consistently come through for us providing reliable, secure and timely IT support. Ryan Haislar and his staff have a thorough understanding of the health care environment and **the budgetary constraints of a small business.**

Ryan is able to work with all levels of technological skill, supporting staff with limited IT skill with professionalism and respect. At the same time Ryan's understanding of our business allows him to represent us and our interest with our vendors, this results in successful implementation of new software or services and quick resolutions of problems.

I recommend Ryan Haislar and Computerease without hesitation.

*Suzann M. Crowder, MBA, CMPE, Administrator
St. Charles Orthopaedic Surgery Associates, Inc.
Healthcare Billing of St. Charles*



St. Charles Orthopaedic
SURGERY ASSOCIATES



The game was great, I have never been to the UMB Champions Club and it was very nice!

Computerease Flashback: Ike Haislar - Radio Talkshow Host 1988-1998

Every Saturday morning from 10am-noon for 10 years, Ike Haislar, founder of Computerease, hosted a radio talk show about all things computers that aired on the local WRYT 1080 AM station.



Why did you start a radio show?

There wasn't another show locally or even nationally that covered computers – and businesses were starting to use technology more and more in their day-to-day operations. Our target audience was business professionals who used a single computer and even multi-user networks. We averaged 2,000-3,000 people listening for a specific segment and even had Toshiba, HP and AT&T executives as guests!

What is your best memory of producing this show?

It was just a great experience! We laughed, we had fun and it was enjoyable. We were constantly doing something silly while helping people at the same time.

How has business changed since you started Computerease in 1984?

The biggest change has been our transition from a break-fix company that built and fixed individual computers to an IT managed service provider for small and medium businesses that depend on reliable IT support, data back-ups and cybersecurity solutions. My son, Ryan, is now the Vice President of Computerease and he has worked very hard to serve our local St. Louis business owners with all of the latest technology advantages and needs. I'm very proud of what he has accomplished!

*Get More Free Tips, Tools and Services At: www.computer-service.com
(314) 432-1661 (MO) or (618) 346-8324 (IL)*

■ NEVER Throw Your Boarding Pass Away, Not Even After Your Flight

Everybody knows that a boarding pass is mandatory in order to board a plane. While we're in the airport, we keep a close eye on our boarding passes, clutching them in our hands like they're precious gems. But after we land, pretty much everyone ditches the ticket, whether it's lost on the floor, compacted in the washing machine or thrown directly into the trash.

This may seem innocent enough, until you realize the abundance of personal information encrypted on your pass. You'd be amazed

at the information a person can glean just by scanning the QR code on the ticket: your home and e-mail addresses, your phone number and even your bank information! When you get rid of your next boarding pass, shred it. Your bank account will thank you.

LuxuryAndGlamor.com
2/5/2016

■ Are You Missing This One Critical Component In Your Business? If So, You Are GUARANTEED To Be Losing Sales As Inc. writer

Rohit Arora puts it, "It may be 2017, but many companies are still conducting business like it's the 20th century." According to data collected in a recent CNBC report, close

to half of small businesses don't even have a website, and even fewer — around 36% — use a website to stay in touch with their customers and prospects. But if we can learn something from Nick's Pizza & Deli in New Jersey, it's that even the smallest companies can leverage new technologies to dramatically increase sales. The restaurant



partnered with a company called The Block, a business that builds websites for small businesses, granting them online ordering capabilities. As a result, Nick's owner estimates an increase in annual revenues of around 15% to 20% in only six months. When you make it easy for your customers to pay, you drive further sales. It's that simple. *inc.com*
8/6/2017

Who Else Wants To Win A Fun Prize?

The Grand Prize Winner of last month's Trivia Challenge Quiz is Anne from Clayton, MO! She was the winner from the drawing of people who submitted correct answers for my quiz question from last month.

Which American president made a note in his diary that he "went to Alexandria to a barbecue?"

- a) Thomas Jefferson b) James Monroe c) Abraham Lincoln
- d) George Washington

The correct answer was b) George Washington.

Now, here's this month's trivia question. The winner will receive 4 tickets to Boo At The Zoo!

Which St. Louis landmark is said to be haunted?

- a) Lemp Mansion b) Cathedral Basilica c) Old St. Louis Courthouse
- d) Field House Museum

***Submit your response to answer@computer-service.com!
Everyone who answers correctly will be placed in the drawing to win our fun prize!***