Technology Today

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

How do you celebrate?

There are a ton of options for celebrating St. Patrick's Day including dyeing a river green, attending a parade, having a pint of Guinness or making your favorite "traditional" corned beef and cabbage meal. An internet search for corned beef and cabbage recipes brings up 425,000 options to make a delicious meal!

There is obviously not one "right" way to make this time-honored dish, you can pick the version that you think sounds best to your tastes.

Similarly, the same technology solution will not be well-suited for every business. There are limitless combinations and numerous factors to consider when creating a customized IT solution.

When working with current and prospective clients, we take the time to listen and learn about how your business works and what is most important to you. Together we will find that perfect recipe for how technology works for your business.

March 2021

This monthly publication provided courtesy of Ryan Haislar, 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!"

Breakdown Of An Almost-Disastrous, Highly Targeted Email Phishing Attack

It's most common to hear stories about businesses falling victim to a cyberattack and the devastating aftermath involved. This is a different type of story. It's a detailed account of how a proactive cybersecurity solution, email SPAM filtering, saved the day for one of our clients targeted by an email phishing attack. Here's the details of how it all worked.

Hacked email at a vendor: A hacker breached the email account of one employee at a vendor of our client (our client's email was not breached). We'll refer to this vendor employee as Employee A. The hacker read through many different emails in Employee A's account and determined which contacts would be most valuable to target.

Hacker studied emails looking for his victims: Then, the hacker took time to carefully craft emails to Employee A's key contacts that would be the most lucrative. This list included one of our client's employees, we'll refer to this person as Employee B. It's important to realize that Employee A and Employee B have a long-standing history of working together and corresponding mostly by email about important matters regarding finances and employee data.

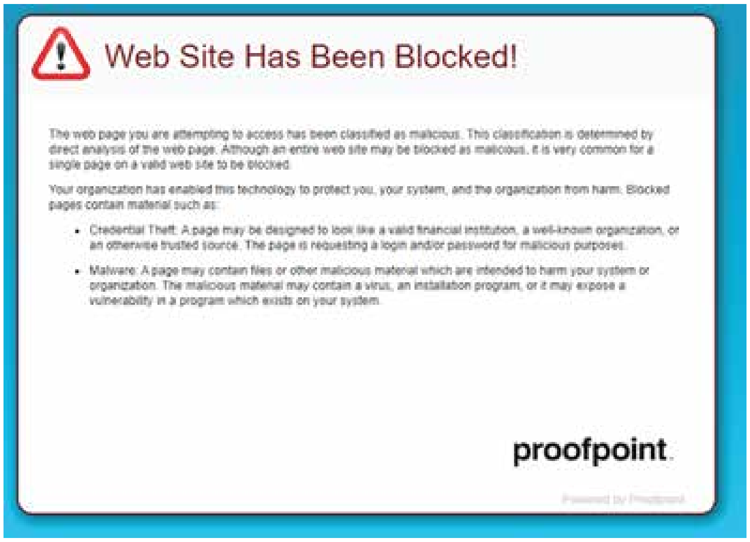
Hacker carefully writes a phishing email: With a simple search of the compromised vendor email account for Employee A, the hacker knows the language and topics commonly emailed between vendor Employee A and our client Employee B. Since the hacker has access to the complete email history between these two individuals, writing a convincing email is very easy. The only real difference between a legitimate email and the hacker's version is one link. The hacker replaces a single link within the email from

<continued page 2>

<continued from page 1> from Employee A to Employee B with a malicious link. The goal of the hacker's email to Employee B is to convince Employee B to click on the malicious link, thereby infecting Employee B's computer.

Target is tricked by phishing email: Because the hacker has control of Employee A's email mailbox on an otherwise legitimate, trusted and spam-free email domain, the hackers email passes the initial spam filter tests for legitimacy and is delivered. Employee B received the fake phishing email sent by the hacker, and because of their relationship with the now hacked Employee A, clicked on the malicious link. Why not, right? There were no red flags for Employee B. Employee A is a trusted and known person that sends regular emails. This most recent email was seemingly just another typical business email. This is exactly what makes this type of email so incredibly dangerous!

Target clicks on link in phishing email: Employee B clicked the link in the email. Here's the message Employee B saw on her screen after clicking the malicious link.



Web Site Has Been Blocked!

The web page you are attempting to access has been classified as malicious. This classification is determined by direct analysis of the web page. Although an entire web site may be blocked as malicious, it is very common for a single page on a valid web site to be blocked.

Your organization has enabled this technology to protect you, your system, and the organization from harm. Blocked pages contain material such as:

- Credential Theft: A page may be designed to look like a valid financial institution, a well-known organization, or an otherwise trusted source. The page is requesting a login and/or password for malicious purposes.
- Malware: A page may contain files or other malicious material which are intended to harm your system or organization. The malicious material may contain a virus, an installation program, or it may expose a vulnerability in a program which exists on your system.

SPAM email filter catches malicious link, disaster avoided: Employee B called us because she thought there was a problem and she needed to get the information in the malicious email from Employee A. We quickly looked into her problem and we were surprised with what we found. We realized that the link and email sent to Employee B at our client's office was a highly targeted phishing email. Then, we celebrated when we realized that our email SPAM filter had worked exactly as designed to prevent disaster!

Hacking activities discovered: We advised Employee B that this was in fact a fake phishing email and that the link was malicious. A short while later, Employee B received a call from the vendor and Employee A stating that her email account had been hacked. The hacker had been sending out fake phishing emails for at least a few hours, including the one sent to Employee B at my client's office.

Here's what could've happened: Luckily for our client, we do have a number of other security layers in place which are designed to stop infections from these types of malware. Normally, the combination of these other layers is highly effective and likely the clients attempt to click on the malicious email link would have been blocked by their firewall, DNS filter or our advanced endpoint protection platform. However, cybersecurity is a cat and mouse game of sorts. Hackers just need to find one way to get their foot in the door, and if they do, it can be game over for the hacker's victim.

For a company which is not as well protected as our client was, this situation would likely have ended very badly. They could have been compromised with ransomware which locked their entire computer or company network. They could have banking credentials stolen which could lead to tens or hundreds of thousands of dollars being siphoned from their business bank accounts. If they were in the healthcare industry, they could have had patient data stolen and been subject to significant government fines. These are just a sampling of what could have happened if a client was not using the types of security measures that we recommend. If you are not confident that your business or organization is secure from cyber thieves, contact us for a free security assessment.

Sign Up for Our FREE "Cybersecurity Tip of the Week" And Always Stay One Step Ahead of Hackers and Cyber-Attacks!

Cyber criminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life.
Start fighting cybercrime with KNOWLEDGE & ACTION!
No Catch. No Obligation.
Just week after week of timely tips to keep you one step ahead of hackers.

Sign up today at: www.computer-service.com/cybersecurity-tips

Shiny New Gadget Of The Month:

Sticker — The Smallest Finder By Tile

First, there was the Tile – a small, square device used to find just about anything. You attach Tile to the thing you don't want to lose (keys, for example) and you pair Tile with the Tile app. Easy!

Now, Tile has introduced Sticker, their "smallest finder." It's a mini-version of their popular fob, and it can be stuck to just about anything, from TV remotes and portable electronics to tools, bikes, you name it – anything you don't want to go missing.

Plus, not only does Sticker stick to anything, but it also has a three-year battery life, so as they say, "you can set it and forget it." Once it's paired with the smartphone app, it's super-easy to track. And if you lose a "Stickered" device, Sticker emits a loud ring to help you locate your misplaced item, at a range of about 150 feet. Learn more about Sticker at **TheTileApp.com/en-us/store/tiles/sticker**.

Making & Keeping Customer Connections In A Digital Era

Make the value that you give your customers so high it doesn't matter what the price is. Based on the experiences your brand consistently delivers, your customers should have no idea what your competition charges. You don't need to raise your prices. You need to bring value and better service. This includes employee training – and be sure they understand how to build and keep relationships.

3 Strategies To Dominate The Relationship Economy

- Use technology to allow employees to focus on what's most important: building relationships that result in higher customer loyalty.
- Build a culture that creates emotional connections with your employees.
- Create relationship-building training for new and existing employees.

Things That CAN Be Trained:

- Authenticity
- Insatiable curiosity
- Incredible empathy
- Great listening skills

The 1 Thing That CANNOT Be Trained:

- The ability to love people

Let's focus on what can be trained and what these traits look like.

Authenticity:

- You love what you do, and it's obvious.
- You're transparent – if you have bad news, don't hold it back.
- You are as committed to the success of your customer as they are.
- You know your clients' top three goals for the year.
- Your customer should not be able to imagine a world without your business in it.

Insatiable Curiosity:

- You're dying to learn about others.
- You want to know about both familiar and unfamiliar subjects.
- You're willing to meet as strangers but leave as friends.

Incredible Empathy:

- You look at things from the customer's perspective.
- You put yourself in your customer's shoes.
- You listen and think from the other person's point of view, allowing their message to become much clearer.
- You're wary of empathy fatigue and able to reset yourself.

Great Listening:

- You give them fierce attention.
- You ask a question and then more questions.
- You don't defend questions and instead explore new ones.
- You bounce questions back.
- You fight the urge to reply before you finish listening.

Every employee should possess these four traits, and you should be willing to train your team to deliver on these traits. When you successfully bring these four elements together, you are set up for success and have the foundation to build and maintain strong relationships with your customers.

Leah Tobak is a Project Manager with Petra Coach. With a background in public relations and marketing, she's done a lot of work building relationships with customers and prospective customers. Outside of the corporate landscape, Leah is an international model and is known for her work in front of the camera.

Top 4 Security Certifications You Should Have In 2021

GIAC Security Essentials (GSEC)
Ideal for those who may not have an extensive background in IT security and networking but who work in an IT security (or similar) role and want a baseline certification. No prerequisites. Learn more at **GIAC.org/certification/security-essentials-gsec.**

(ISACA) Certified Information Security Manager (CISM)
Less technical and more managerial. Ideal for those in IT and risk management roles that are not strictly technical. Prerequisites for certification include five years experience in information security (including three years as an information security manager). Learn more at **ISACA.org/credentialing/cism.**

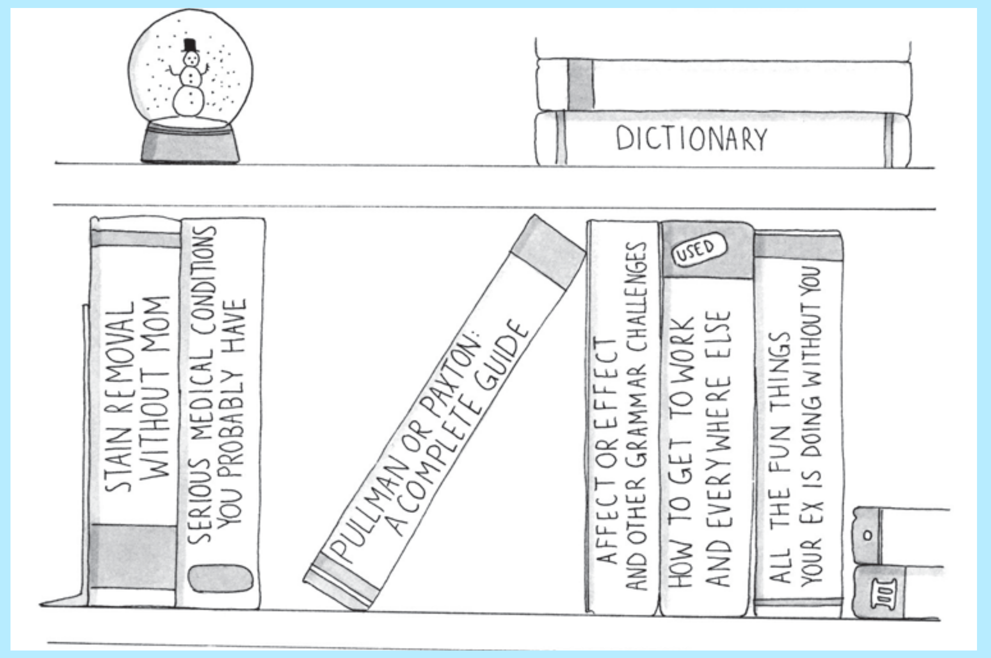
(ISC)² Certified Information Systems Security Professional (CISSP)
A high-level certification aimed at those with an extensive and knowledgeable IT security background. This certification is in very high demand by companies around the world. Prerequisites include five years experience in a position related to CISSP (or one year of experience plus a four-year degree). Learn more at **ISC2.org/certifications/cissp.**

(ISC)² Certified Cloud Security Professional (CCSP)
Ideal for those experienced in IT security with an emphasis on cloud-based solutions. Prerequisites for certification include a minimum of five years of full-time IT experience (with three years in information security). Learn more at **ISC2.org/certifications/ccsp**.
Infosec, Dec. 22, 2020

The Scientific Reason Your Employees Value Opinions Over Facts

The research is clear: people have a habit of putting more value on opinion rather than fact. It's because it's easy! This is discussed in Daniel Kahneman's best-selling book, *Thinking, Fast And Slow*, and in numerous research papers. Accepting opinions requires less thinking than evaluating facts. Data-driven companies need to take this into account when it comes to their teams. According to Kahneman, some people are "type 1" thinkers or fast thinkers, and opinions mean more to them. Others are "type 2" or slow thinkers – they take their time and evaluate what they hear.

Michael Schrage, research fellow at MIT Sloan School's Center for Digital Business, says you can't just switch between the two types of thinking automatically. It's more fundamental – you have to change people's mindsets over time. His suggestion is to incentivize analytical, fact-based thinking and recognize employees who take this approach. *Inc., Oct. 29, 2015*


DICTIONARY
STAIN REMOVAL WITHOUT MOM
SERIOUS MEDICAL CONDITIONS YOU PROBABLY HAVE
PULLMAN OR PAXTON: A COMPLETE GUIDE
AFFECT OR EFFECT AND OTHER GRAMMAR CHALLENGES
USED
HOW TO GET TO WORK AND EVERYWHERE ELSE
ALL THE FUN THINGS YOUR EX IS DOING WITHOUT YOU

3 Simple Yet Effective Ways To Boost Employee Morale

1. Focus On Mental Health. Whether it's your own mental health or the mental health of anyone on your team, make sure everyone has the time and space they need to take a break and refocus their energy. Make sure anxiety and stress are recognized and addressed in a positive way.

2. Be With Your Team. Simply being present and available for everyone on your team goes a long way. Have regular one-on-one chats just to see how things are going and to ask if they need anything. When they do need something, do what you can to help (and be sure to follow up).

3. Recognize Your Employees. Recognize their work and reward them. Everyone should be aware of the effort individuals and teams put into their work. At the same time, make sure they have ownership over their work and give credit where credit is due. *Inc., Nov. 4, 2020*