NOV 2021, ISSUE 2

INNOVATORS PLUS

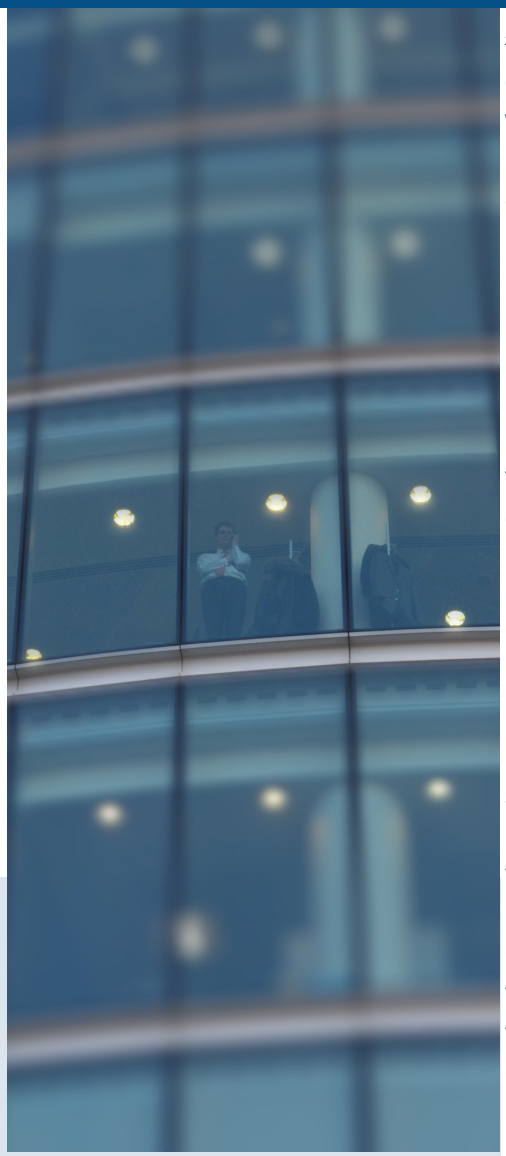
The Monthly Plus 1 Technology Newsletter

WHY AVOIDING CYBER SECURITY TRAINING COULD COST YOU YOUR BUSINESS

Marc Umstead, President

By now, most leadership has heard of cyber security training, but why is it so important? Cybercrime is up 600% due to the Covid-19 pandemic. Almost 90% of all data breaches are caused due to human error. Your company's data is only as strong as your least educated employee. We believe this type of training not only improves your employee's education but can save your business. There are 5 reasons we believe cyber security training can save your business.

WHAT'S INSIDE THIS ISSUE:



#1 Prevents cyber attacks from happening. Since your employees and humans overall are the weakest link, providing them some education on the dos and don'ts when it comes to security provides a durable protection. The training reviews items such as how to spot a phishing email, what information should not be emailed, and how to identify the target of a link.

#2 Employees are aware of security protocols. Educated employees are more likely to practice good password hygiene, be more careful clicking links, and be more conscience of data security.

#3 Maintain your customers' trust. If your company was to suffer a data breach, you would be required to notify all your clients and vendors that you have potentially leaked their personally identifiable information, proprietary information, financial information, and possibly their client's information. A leak like this can cause your clients to leave and a substantial hit to your brand.

#4 Saves your company money. Ransomware or other cyber attacks can be extremely expensive. Even non-ransomware attacks can lead to loss of clients, lawsuits, disruption in operations, and compromised data. The cost of a cyber breach even for a small company can be in the tens of thousands of dollars or much more.

#5 Helps you differentiate your firm. By showing that your firm is taking security seriously your clients will see that your firm is trustworthy. We often recommend displaying your training certificates so your clients can see that you take the security of their data seriously.

Cyber Security is now a requirement for firms to continue to keep their data and their customer's data secure. The alternative may be the complete loss of your firm. 60% of small businesses that had a cyber attack were out of business within 6 months. Cyber training is not a large investment but can provide exponent rewards and protection.

Ensure You are Making A Great First Impression

Many people don't realize it but initially the only comparison a prospect has between you and your competition is your marketing. If the prospect hasn't received a referral from a trusted resource the only comparison tool, they have is your marketing. This includes your website, search reviews, printed material, and your social media content.

Here are a couple of tips to ensure you are making a good first impression. Make sure your web content is updated and speaks to the PROBLEM of your clients. When clients are searching for a service provider, they don't often want to see pages and pages explaining your solution if they aren't sure you can help with their problem.

Make sure you have as many positive google reviews you can get and make sure they are staggered in time. Also, make sure the reviews are replied to, including the bad ones, professionally.

If you are using direct mail or provide printed material make sure it speaks to the client needs and remove as many "good service", "friendly", and "best" platitudes as you can. Find me one company that doesn't say these things, state what makes you truly different.

Finally, address your social media content. If you haven't posted to Facebook in 2 years, delete it. Social media is only good if you are using it to engage with your clients and prospects. Take 5 minutes a week and say something.

If you do these things, much of your competition isn't, so you will win more prospects and close more deals.

RANSOMWARE: WHY BACKUPS ARE NO LONGER PROTECTION

Marc Umstead

We have all heard of the threat of ransomware and how malicious actors encrypt your files and demand a payment to provide access to your data. Until recently there were two major ways firms protected themselves from the threat of ransomware. The first protection was prevention by implementing a stringent Anti-Virus program to stop the infection from infiltrating the network. The second protection was to have offsite or offline backups. Firms that would be infected with ransomware would often opt to just restore from backups and not pay the ransom. Sadly, the second protection now may be obsolete.

Unfortunately, malicious hacking groups have now realized the monetary value of the privacy of the data may be worth more than the access. These bad actors now after collecting a ransom for providing you your data back, will often look to collect a secondary payment with the promise of not posting or releasing the data they collected publicly. Basically, the bad actors now threaten to release the information in the data they were able to obtain through the ransomware attack. This is extremely concerning for companies with any personal or proprietary data or that fall under a compliance law. Now your decision to pay the ransom would also need to consider the public publishing of your data. This new extortion scheme means using a good backup solution as protection from ransomware is no longer viable.

What should you do? We recommend that clients are using a premium endpoint detection and response application such as Sentinel One, Crowd Strike, or other premium product. These products provide a higher level of protection against Ransomware protections because they are based on behavior instead of a static file list. Many of your traditional anti-virus software such as Norton, McAfee, Webroot, and others are based on a list of file paths and applications that are known as “bad” and they don’t allow them to run. The problem is that they are always behind the curve and rely on thousands of infections before they are identified. Next generation protection looks at what an application is trying to do instead of just its name or location to determine that it shouldn’t run. These next generation products also provide an easy way to rollback file changes and disconnect computers from the network automatically if a ransomware type infection is detected.

We recommend that all companies use this next gen protection to bolster their ransomware prevention. They should also maintain their backup infrastructure to combat hardware failures.

Need additional monitors or privacy when working remotely?

Advance productivity with ThinkReality A3—Lenovo’s versatile smart glasses for business. Ultraportable and comfortable, these augmented reality (AR) glasses create a customized, expanded personal workspace anywhere, from a virtual monitor at home, to guided schematics on the factory floor.

Use ThinkReality A3 to create and customize a virtual monitor at home, a private display in a coffee shop, an immersive schematic or guided workflow on the manufacturing floor, and more. View your sensitive or confidential data without fear of "shoulder surfers"—only you can see your virtual monitor. Multi-monitor and -application workflows can be taxing on a PCs performance, creating a need for heavier performance via multi-threaded CPUs and dedicated GPUs. ThinkPad P Series mobile workstations are the fastest, most powerful laptops in the ThinkPad portfolio, delivering the most efficient, seamless user experience. The list of compatible PCs recommended for use with the ThinkReality A3 PC Edition is growing

Can your PC run Windows 11?

Microsoft announced the release of Windows 11. Windows 11 carries from very specific hardware requirements. If you want to know whether your pc can run Windows 11, download and run the Windows PC Health Check from here: https://aka.ms/GetPCHealthCheckApp
Be sure your double check with your Managed Services Provider before installing Windows 11 on any device.

Always double check with your Managed Services Provider before installing any new Programs or Updates.

Thanksgiving Cocktail

It's smooth, creamy, sweet and rich with nuances of pumpkin and cinnamon! It's cozy, full of flavor and perfect for all your holiday parties or cocktail hour at home!

Ingredients:

2 oz. Pumpkin Spice Vodka
1 oz. Dark Rum
1/2 oz. Half and Half
2 tbs Pumpkin Puree
1 oz. Maple Syrup
1/4 tsp Vanilla Extract
3 Ice Cubes

Glass Rim:
Maple Syrup
Crushed Graham Cracker
1/2 tsp. Cinnamon
1 tbs Granulated Sugar

- **Prepare the Garnish: Crush graham cracker in a Ziploc bag, or food processor, until it resembles sand. Stir in the cinnamon and sugar. Line the rim of a martini glass with maple syrup (I used a thick napkin to apply syrup). Dip/roll in the cracker mix. Set aside.**
- **Prepare the Martini: In a cocktail shaker, combine the ice and remaining cocktail ingredients. Shake vigorously until shaker chilled to the touch.**
- **Serve: Strain and pour cocktail into the prepared martini glass. Garnish with cinnamon stick and nutmeg. Enjoy!**

PLUS ONE TECHNOLOGY

3277 W Ridge Pike Suite B201
Pottstown PA 19464

Inside This Issue