Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: Adath Israel Congregation

The origin of the **Adath Israel Congregation** goes back to the turn of the 20th century when Jewish immigrants from Rumania sought refuge from the strangeness of their new environment in the company of their countrymen. Social gatherings led in the course of time to the desire to pray together on the Holy Days and to establish a congregation of their own.

The birth of the congregation in 1903 allowed families to bond and establish a friendship and comfort with one another that prevails today.

Adath Israel offers religious services, education for children and adults, social functions, and congregational events and activities to about 1600 families, and continues to provide services and support to new congregants.

Connectability has been Adath Israel Congregation's technology partner since 2006. We are responsible for managing their computers, server, and phone systems to ensure the Synagogue can carry out their services and congregational events smoothly. We ensure that their data is secure and confidential, and we have implemented a number of security protections to help minimize their risks of becoming the victim of cyber-attacks. We take care of their IT needs, so they can focus on supporting their congregants, and the Jewish community as a whole!

If you would like to learn more about Adath Israel Congregation, please go to: https://www.adathisrael.com/

November 2020

This monthly publication provided courtesy of Ted Shafran, President of Connectability

4 Questions Your IT Services Company Should Be Able To Say "Yes" To

Out with the old and in with the new! For far too long, small businesses have taken an old-school approach to IT services and security. In other words, they wait until something goes wrong before they call an IT services company and request help.

Back in the day (think 1990s and 2000s), this approach worked, more or less. External threats, such as hackers and viruses, were still few and far between. A data breach wasn't on anyone's mind. So, it made sense to wait until something went wrong before taking action.

In IT circles, this is known as the "break-fix" approach. Something breaks, so someone has to come in to fix it. And they charge for their services accordingly. If something small breaks and it takes a short time to fix, you could expect a smaller bill. If something big breaks, well, you can expect a pretty hefty bill.

The break-fix approach is 100% reactive. As many businesses have learned, especially in more recent years, as the number of threats have skyrocketed, it can get very expensive. IT specialists are an in-demand field. With just about every business relying on the Internet and Internet-connected devices in order to operate, there's a lot of opportunity for something to go wrong.

This is exactly why you can't rely on the reactive break-fix model anymore. If you do, you could be putting your business at serious risk. In some cases, the mounting costs and damages done could put you out of business.

If you're hit by a data breach or if a hacker infiltrates your network (which is a common occurrence), what's next? You call your IT services partner – if

Continued on pg.2

Continued from pg.1

you have a partner – and tell them you need help. They might be able to restore lost or stolen data. That is, if you routinely backed up that data. You don't want to find yourself in this position.

And you don't have to.

Instead, take a proactive approach to your IT support and security. This is the new way of doing things! It's also known as managed services – and it's a far cry from the break-fix approach.

If you work with an IT services company that only comes out when something breaks, it's time to get them on the phone to ask them four big questions. These are questions they absolutely need to say "yes" to.

1. **Can you monitor our network and devices for threats 24/7?**
2. **Can you access my network remotely to provide on-the-spot IT support to my team?**
3. **Can you make sure all our data is backed up AND secure?**
4. **Can you keep our network protected with up-to-date malware solutions, firewalls and web filtering?**

> **"When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!"**

If your IT services partner says "no" to any or all of these questions, it might be time to look for a new IT services partner.

If they say "yes" (or, even better, give you an emphatic "yes"), it's time to reevaluate your relationship with this company. You want to tell them you're ready to take a proactive approach to your IT support, and you'll be happy to have them onboard.

Far too many small businesses don't bother with proactive support because they don't like the ongoing cost (think of it as a subscription for ongoing support and security). They would rather pay for things as they break. But these break-fix services are more expensive than ever before. When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!

Don't be that person. Make the call and tell your IT services provider you want proactive protection for your business. Ask them how they can help and how you can work together to avoid disaster!

You Need To Cover Up Your Webcam With A Sticker!

Here's a disturbing, but very real, tactic for hackers: spying on you via your device's camera. Some simply watch you for fun. Others attempt to catch incriminating photos and then blackmail you by threatening to release the photos or video (which they have) to all your Facebook friends, LinkedIn connections or e-mail address book (which they also have) unless you pay a ransom. If you pay, they can come back and ask for MORE because they now know you care AND that you'll pay. If you don't pay, they will release that picture of you doing, um, well…

As always, follow the various security strategies we've been sending you via these tips. As a backup, you can buy stickers that cover your camera with a slider so you can uncover it when you want to actually use it to take a picture or join a web meeting. These are really inexpensive and can be found on Amazon for under $10. Search for "webcam cover slider."

Shiny New Gadget Of The Month:

Arlo Pro 3 Floodlight Camera

In the era of porch pirates, more people are investing in outdoor security cameras. The Arlo Pro 3 Floodlight Camera delivers security and practicality. It features an ultrahigh-definition camera delivering 2K HDR video and colour night vision combined with a 2000 lumens light. Nothing goes undetected!

Plus, the Arlo Pro 3 is wireless. It connects to WiFi and doesn't need a power cord (it just needs to be plugged in for charging periodically). Because it's on WiFi, you can check the feed anytime from your smartphone. You can even customize notifications so you're alerted when it detects a car or person. And it has a speaker and microphone so you can hear and talk to anyone near the camera. Learn more at:
https://amzn.to/32BQPgc

7 Things To Do So You DON'T Get Hacked When Shopping Online

1. Verify the URL is safe. Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate. Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser. Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

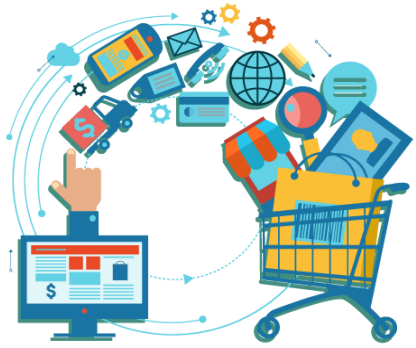
4. Don't click suspicious links or attachments. Never click a link if you can't verify it first. In fact, it's better to delete any e-mail you don't recognize.

5. Always bookmark authentic websites. When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager. It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores. If you download the official app of your favourite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple.

Lifehacker, Nov. 19, 2019.



Tech Connect Video Series:
Multi Factor Authentication Is More Important Now Than Ever!

Cybercrime is on the rise. Hackers are using all the tools and resources at their disposal to find your login credentials, access your accounts, and steal your company and personal data. Most people tend to use weak, easy-to-guess passwords (like birthdays and pet names) or use the same password for all their accounts. By using simple passwords, you can be a victim of a security breach. That's why it's important to have an additional layer of protection to put a stop to hackers.

MFA immediately increases your account security by requiring multiple forms of verification to prove your identity when signing into an application. By using multi-factor authentication (MFA), you make it more difficult for cybercriminals to exploit and obtain your sensitive data – even if they have your password.

Watch this video to learn 3 benefits of multi-factor authentication and how it can protect you and your business from a cyber-attack. To find out more, goto YouTube, look up Connectability IT Support and find the video **"Multi Factor Authentication Is More Important Now Than Ever!"** OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

Is Working From An Office More Secure Than Working Remotely?

It may come as a surprise, but working remotely can be just as (or more) secure than working in the office. If done right.

Those are the three operating words: if done right. This takes effort on the part of both the business and the remote employee. Here are a few MUST-HAVES for a secure work-from-home experience:

Secure networks. This is non-negotiable. Every remote employee should be connecting to a secure network (at home, it should be WPA2 encrypted), and they should be doing so with a VPN.

Secure devices. All devices used for work should be equipped with endpoint security – antivirus, anti-malware, anti-ransomware and firewall protection. Employees should also only use employer-provided or approved devices for work-related activity.

Secure passwords. If employees need to log in to employer-issued programs, strong passwords that are routinely updated should be required. Of course, strong passwords should be the norm across the board. *Entrepreneur, June 17, 2020*

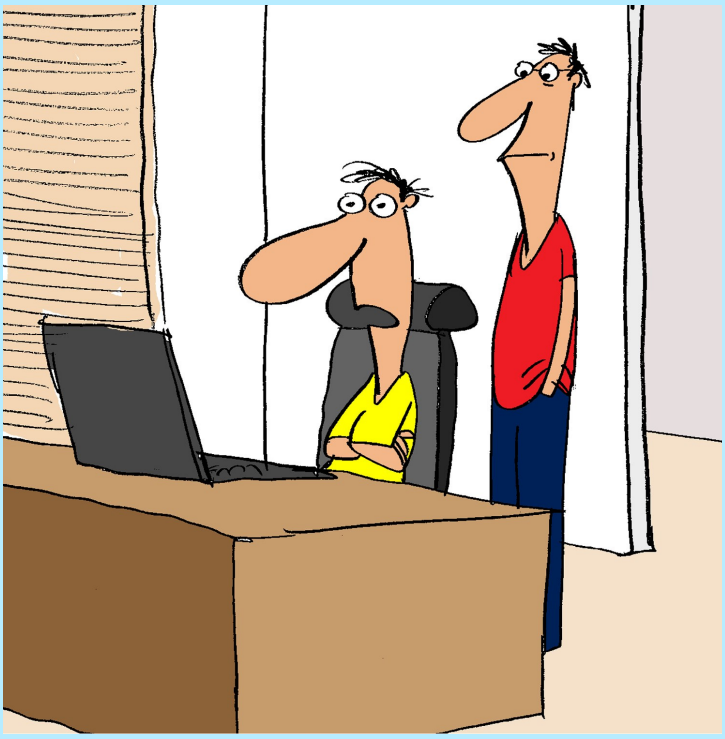
Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1. Regularly update your passwords. Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

2. Say no to sharing. Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

3. Connect the camera to a SECURE network. Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better. *Digital Trends, May 7, 2020*



"This figures. My file on politicians has become corrupt."

This month we will be donating to **Soldier On**.

Founded in 2007, Soldier On is a program of the Canadian Armed Forces Transition Group. Soldier On is committed to providing support for veterans and serving members to help adapt and overcome permanent physical injury or PTSD.

Soldier On is dedicated to improving the quality of life of veterans and current serving members through physical activity and sport. Soldier On provides a safe environment and empowers them to adapt and re-integrate with local, community-based activities, and remain active for life.

If you want to contribute to Soldier On, we would love your help! Email: info@connectability.com or call (647) 492-4406.