MAKE I.T. EASY

Insider tips to make your business run faster, easier, and more profitably.

CYBERSECURITY AWARENESS MONTH

Use a strong password to protect your candy.

The scariest threat might be your employees. Invest in security training.

Look through the masks that cyber criminals wear to trick you. Think before you click.

The internet of evil things: many internet connected devices have security flaws.

In our connected world, it seems like cybercriminals and malicious links creep around every corner. News stories of ransomware attacks and data breaches costing millions of dollars fly past our feeds almost constantly.

The thought of keeping your business secure can be overwhelming. That's why we're recognizing Cybersecurity Awareness Month this October by sharing tips to stay cyber secure, both at work and at home. A little knowledge with critical thinking skills can go a long way in building your defense.

Just Solutions is committed to educating our business community. Cybersecurity is not a trend that will be going away anytime soon. You owe it to your employees, customers, clients, and yourself to protect your business data. If you have any questions, feel free to contact us at **sales@justinc.com**.

WHAT'S NEW IN CYBERSECURITY

With David Wolf, Vice President of Just Solutions Inc.

ZERO! "Well, that is "zero trust", I mean.

We humans are so trusting. We trust our parents, our teachers, our clergy, our scientists, and even our politicians. Really?!

With all the news articles regarding abuses and unforgivable actions by all the above authority figures in our lives, I am amazed that people are still so trusting of emails, text messages, phone calls from people they do not know or are acquaintances.

The consensus in cybersecurity is to stop trusting anything or anyone and verify every transaction or request. You will read more and more about "zero trust" and programs that assist you with this new security concept. It is pretty simple to follow - do not trust any user and verify everyone or any device you use, connect to, or communication with. Bring your own device (BYOD) is an absolute no-no with zero trust. If the device is not managed and secure, how can you trust it? Work from home (WFH) exacerbates this issue with people using home computers or networks that are not well protected or maintained.

Zero trust also means verification and validation of internal users and devices. Do you have open ports in the office that anyone can plug into and get a connection? Do you share your Wi-Fi password? I see Wi-Fi passwords posted in offices all the time. Does your system monitor and alert when new devices are plugged in and connected? Does anyone pay attention? All these situations help demonstrate why zero trust is necessary.

Email accounts are compromised (hacked) every day. Why? Passwords are weak or easily cracked. "Zero trust" says use an additional verification step to confirm identity. Send a text code to a predetermined phone, require a pin from an authorization app or "fob", or call and phone verify personal information.

Is the attempted login originating from a local internet connection or location that is approved? Or is it coming from North Korea or China? "Geofencing" - the use of location tools to block unusual locations, is a way "not to trust" the original request when something does not make sense geographically. Think about the time your credit card got blocked when you were traveling out of state. The credit card company wanted to make sure your credit card was not lost or stolen.

What is the Microsoft Zero Trust Framework?

"Microsoft has adopted a modern approach to security called “zero trust,” which is based on the principle: never trust, always verify. This security approach protects our company and our customers by managing and granting access based on the continual verification of identities, devices and services." This quote is from Microsoft’s website.

I am sure you are getting more frequent prompts to login and verify your Microsoft sign-on with Office 365. Microsoft will alert you of unusual account activity as well. Third party companies have solutions to monitor this activity across all of your devices and software applications.

Zero Trust also requires not giving administrative permissions to users and not letting admins use their admin account for daily routine tasks. "Hardening" just means tightening up security, turning off unnecessary services and access, and 24x7 monitoring of all activity.

Network isolation and separation is another principle and tactic used to create a zero trust environment. The major Target breach occurred because the HVAC system controls where on the same network as the point of sale system. By getting into the HVAC system, hackers were able to connect to the credit card systems. Today, isolation and virtual LANS (Vlans) are not just for Voice and Data. They can be used to separate the “Internet of Things” (IoT) connected devices. Cameras, thermostats, refrigerators, door locks and hundreds of other WIFI connect devices which should not be sharing your primary data network.

The Real Treat Is Staying Cybersecure All Year Long.

NEED A SECURITY ASSESSMENT?

Book An Appointment