SOLUTIONS
MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

MONTHLY UPDATE FROM TROY

Let's talk about ditching the manual grind for a second – automating things is like giving your workload a magic wand. Seriously, who needs to spend hours doing repetitive tasks when we've got tech that can do it like a champ?

Whether it's sorting through emails, handling data entry, or whatever your daily hustle involves, automation is the superhero that swoops in to save you time and sanity. Plus, fewer chances of data errors – bonus! So, next time you're stuck in a manual maze, think automation. Your productivity levels will thank you!

Need some help automating manual processes? Reach out to us at info@solve-it-sol.com to schedule a chat.

Until then, stay safe,

Troy Kantner
Founder / President / CEO

DID YOU KNOW?

The word technology was coined in 330 BC by the one and only Aristotle.

f /SOLVEITSOLUTIONS

🐦 /solveitsol

in /company/solve-it-solutions-llc

📷 /solveit_sol

02

BE CAREFUL WHEN SCANNING QR CODES

QR codes are everywhere these days. You can find them on restaurant menus, flyers, and posters. They're used both offline and online. QR codes are convenient and easy to use. You just scan them with your smartphone camera. You're then directed to a link, a coupon, a video, or some other online content.

With the rise in popularity of QR codes comes an unfortunate dark side. Cybercriminals are exploiting this technology for nefarious purposes. Scammers create fake QR codes. They can steal your personal information. They can also infect your device with malware or trick you into paying money.

It's crucial to exercise caution when scanning QR codes. This emerging scam highlights the potential dangers lurking behind those seemingly innocent squares.

QR codes were originally designed for tracking parts in the automotive industry. They have experienced a renaissance in recent years as a result, they're used as a form of marketing today.

They offer the convenience of instant access to information. You simply scan a code. Unfortunately, cybercriminals are quick to adapt. A new phishing scam has emerged, exploiting the trust we place in QR codes.

MENU

OPEN YOUR CAMERA APP
SCAN THIS QR CODE TO SEE OUR MENU
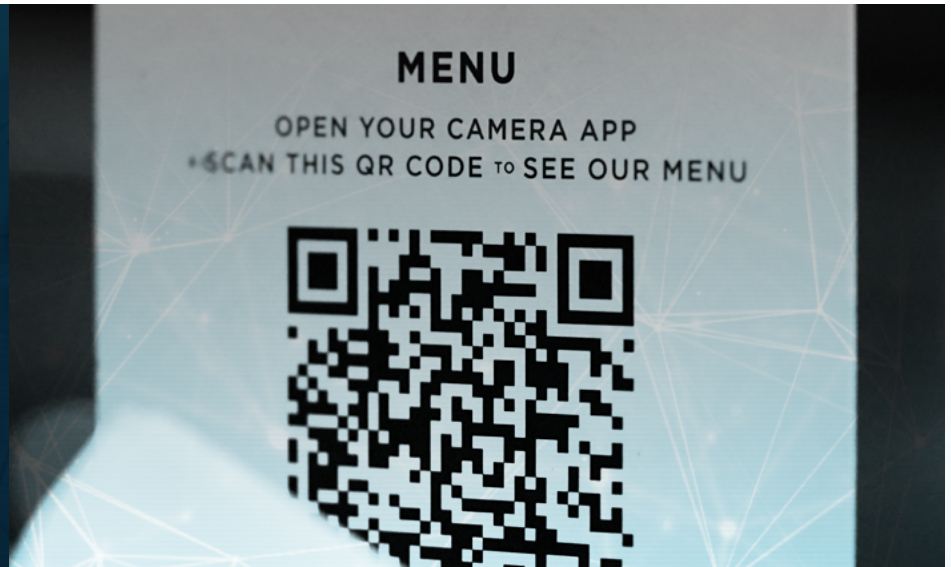
How the Scam Works

The scammer prints out a fake QR code. They place it over a legitimate one. For example, they might stick it on a poster that advertises a product discount or a movie.

You come along and scan the fake QR code, thinking it's legitimate. The fake code may direct you to a phishing website. These sites may ask you to enter sensitive data such as your credit card details, login credentials, or other personal information.

Or scanning the QR code may prompt you to download a malicious app. One that contains malware that can do one or more of the following:

- Spy on your activity
- Access your copy/paste history
- Access your contacts
- Lock your device until you pay a ransom

The code could also direct you to a payment page. A page that charges you a fee for something supposedly free.

Here are some tactics to watch out for:

Malicious Codes Concealed
Cybercriminals tamper with legitimate QR codes. They often add a fake QR code sticker over a real one. They embed malicious content or redirect users to fraudulent websites.

Fake Promotions and Contests
Scammers often use QR codes to lure users into fake promotions or contests. When users scan the code, it may direct them to a counterfeit website.

Malware Distribution
Some malicious QR codes start downloads of malware onto the user's device.

Stay Vigilant: Tips For Safe QR Code Scanning

Verify the Source
Verify the legitimacy of the code and its source.

Use a QR Code Scanner App
Use a dedicated QR code scanner app rather than the default camera app on your device.

Inspect the URL Before Clicking
Before visiting a website prompted by a QR code, review the URL.

Avoid Scanning Suspicious Codes
Trust your instincts. If a QR code looks suspicious, refrain from scanning it.

Update Your Device and Apps
Keep your device's operating system and QR code scanning apps up to date.

Be Wary of Websites Accessed via QR Code
Don't enter any personal information on a website that you accessed through a QR code. This includes things like your address, credit card details, login information, etc. Don't pay any money or make any donations through a QR code.

03   WHAT IS MICROSOFT SECURITY COPILOT?

It can be challenging to keep up with the ever-evolving cyber threat landscape. Companies need to process large amounts of data. As well as respond to incidents quickly and effectively. Managing an organization's security posture is complex.

That's where Microsoft Security Copilot comes in. Microsoft Security Copilot is a generative AI-powered security solution. It provides tailored insights that empower your team to defend your network. It also works with other Microsoft security products.

Microsoft Security Copilot helps security teams:
- Respond to cyber threats
- Process signals
- Assess risk exposure at machine speed

A big benefit is that it integrates with natural language. This means you can ask questions plainly to generate tailored guidance and insights. For example, you can ask:
- What are the best practices for securing Azure workloads?
- What is the impact of CVE-2024-23905 on my organization?
- Generate a report on the latest attack campaign.
- How do I remediate an incident involving TrickBot malware?

Security Copilot can help with end-to-end scenarios such as:
- Incident response
- Threat hunting
- Intelligence gathering
- Posture management
- Executive summaries on security investigations

How Does Microsoft Security Copilot Work?

You can access Microsoft Security Copilot capabilities through a standalone experience as well as embedded experiences available in other Microsoft security products.

Copilot integrates with several tools, including:
- Microsoft Sentinel
- Microsoft Defender XDR
- Microsoft Intune
- Microsoft Defender Threat Intelligence
- Microsoft Entra
- Microsoft Purview
- Microsoft Defender External Attack Surface Management
- Microsoft Defender for Cloud

You can use natural language prompts with Security Copilot.

Should You Use Microsoft Security Copilot?

The Pros:
- Advanced Threat Detection
- Operational Efficiency
- Integration with Microsoft Products
- Continuous Learning
- Reduced False Positives

The Considerations:
- Integration Challenges
- Resource Requirements
- Training and Familiarization

The Bottom Line

Microsoft Security Copilot represents a leap forward in the realm of AI-driven cyber security.

It has an advanced capacity for real-time threat detection and operational efficiency as well as extensive integration capabilities. These factors make it a compelling choice especially for businesses seeking to fortify their digital defenses.

Your unique business needs should guide the decision to adopt Microsoft Security Copilot. Consider factors such as existing cyber security infrastructure and resource availability as well as the commitment to ongoing training.

04   TACTICS TO REDUCE CLOUD WASTE AT YOUR BUSINESS

Cloud computing has revolutionized the way businesses operate. It offers scalability, flexibility, and cost-efficiency. But cloud services also come with a downside: cloud waste.

Cloud waste is the unnecessary spending of resources and money on cloud services. These services are often not fully utilized or optimized. About 32% of cloud spending is wasted.
This can lead to budget concerns as spending skyrockets.

But that figure also holds opportunity. It means that you can reduce nearly a third of cloud spending by optimizing how you use cloud tools.

Here are some smart tactics to reduce cloud waste and save money:

Conduct a Comprehensive Cloud Audit
Before implementing any cost-cutting strategies, conduct an audit.

Put in Place Right-Sizing Strategies
Analyze your workload requirements and resize instances accordingly.

Use Reserved Instances and Savings Plans
Cloud providers offer cost-saving options like Reserved Instances (RIs) and Savings Plans.

Install Automated Scaling Policies
Dynamic workloads have a need for dynamic resource allocation. Install automated scaling policies.

Track and Optimize Storage
Regularly review and delete unnecessary data to free up storage space.

Schedule Your Cloud Resources
Schedule your cloud resources to run only when you need them.

Delete Unused or Orphaned Cloud Resources
Regularly audit your cloud environment to delete any unused or orphaned resources your business is not using.

Weed Out Duplicate Services
Centralize cloud resources and remove duplicate tools.

Embrace Serverless Architecture
Serverless computing allows businesses to run applications without managing the underlying infrastructure.

501 N Park Road | Wyomissing, PA 19610 | 484.331.1083   **www.solve-it-sol.com**

05

CYBER SECURITY PREDICTIONS FOR 2024 YOU SHOULD PLAN FOR

Cyber security is a constantly evolving field. There are new threats, technologies, and opportunities emerging every year. As we enter 2024, organizations need to be aware of current and future cyber threats. Businesses of all sizes and sectors should plan accordingly.

Staying ahead of the curve is paramount to safeguarding digital assets.

5 cyber security predictions for 2024 that you should consider:

1. AI Will Be a Double-edged Sword
2. Quantum Computing Will Become a Looming Threat
3. Hacktivism Will Rise in Prominence
4. Ransomware Will Remain a Persistent Threat
5. Cyber Insurance Will Become More Influential

06

9 SIGNS THAT YOUR SMART DEVICE HAS BEEN HACKED

Smart IOT devices are becoming more popular and convenient. But they also pose some serious security risks. Hackers can target these devices to access your personal information. As well as spy on your activities or cause damage to your office.

How can you tell if a hacker has compromised your smart IOT device? Here are some signs to look out for.

- Unexpected Behavior
- Unusual Network Traffic
- Strange Sounds or Voices
- Device Settings Modification
- Unexplained Data Transfers
- Device Inaccessibility
- New or Unknown Devices on the Network
- Frequent Software Glitches
- Emails or Messages Confirming Changes You Didn't Make

07

EYE-OPENING INSIGHTS FROM THE 2023 ANNUAL CYBER SECURITY ATTITUDES AND BEHAVIORS REPORT

Often, it's our own actions that leave us most at risk of a cyber attack or online scam. Risky behaviors include weak passwords and lax security policies and also thinking, this won't happen to me.

The National Cyber security Alliance and CybSafe published a report on cyber security attitudes and behaviors. The goal is to educate both people and businesses. The report reveals some eye-opening insights.

Here are some of the key findings from the report:

- We are online a lot: 93% of respondents are online daily.
- We store sensitive stuff online: 47% of respondents have ten or more sensitive online accounts.
- Online security makes people frustrated: 39% of people feel frustrated when trying to stay safe online.
- People need more access to training: Just 26% of the survey respondents had access to cyber security training.