SOLVE
IT SOLUTIONS

ISSUE: 2 | APRIL 2023

SOLUTIONS MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

MONTHLY UPDATE FROM TROY

Is privacy truly lost in today's world? It may seem that way when you find out apps like Facebook are tracking all digital purchases you make on 3rd party sites. But there are things you can do to better protect your data.

Whether you're worried about your individual information or business data, protecting online privacy just takes more knowhow these days.

For instance, many apps allow you to turn off tracking features they enable by default. But you have to know where to do it. There are also many digital tools you can use to block unwanted tracking and data leakage.

Email us at info@solve-it-sol.com to schedule a chat and a data privacy checkup.

Until then, stay safe,

Troy Kantner
Founder / President / CEO

WHAT'S INSIDE?

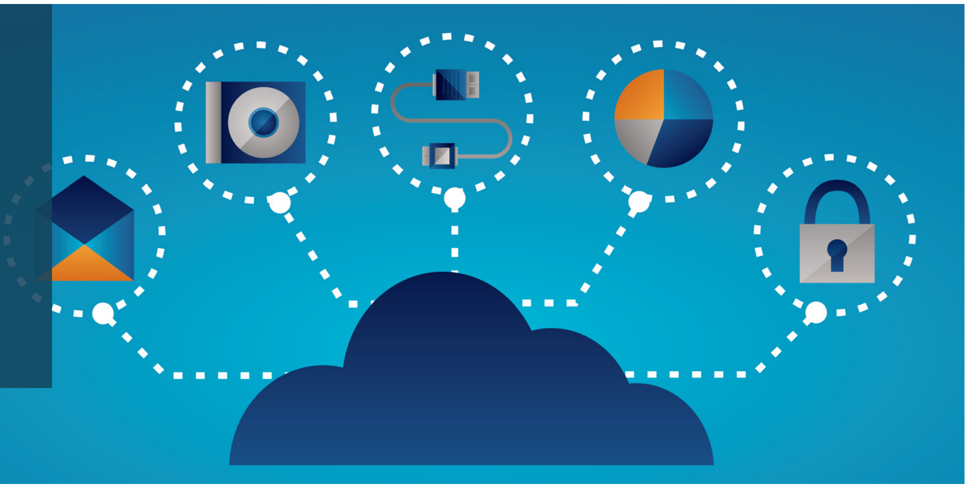
DID YOU KNOW?

The first modern digital virtual assistant installed on a smartphone was Siri, introduced as a feature of the iPhone 4S on 4 October 2011.

/SOLVEITSOLUTIONS
/solveitsol
/company/solve-it-solutions-llc
/solveit_sol

02

DATA BACKUP IS NOT ENOUGH



- The need to back up data has been around since floppy disks. Data loss happens due to viruses, hard drive crashes, and other mishaps. Most people using any type of technology have experienced data loss at least once.
- There are about 140,000 hard drive crashes in the US weekly. Every five years, 20% of SMBs suffer data loss due to a major disaster. This has helped to drive a robust cloud backup market that continues to grow.
- But one thing that's changed with data backup in the last few years is security. Simply backing up data so you don't lose it, isn't enough anymore. Backing up has morphed into data protection.

WHAT DOES THIS MEAN?

It means that backups need more cybersecurity protection. They face threats such as sleeper ransomware and supply chain attacks. Cloud-based backup has the benefit of being convenient, accessible, and effective. But there is also a need for certain security considerations
with an online service.

Companies need to consider data protection when planning a backup and recovery strategy. The tools used need to protect against the growing number of threats.

Some of the modern threats to data backups include:

Data Center Outage: The "cloud" basically means data on a server. That server is internet accessible. Those servers can crash. Data centers holding the servers can also have outages.

Sleeper Ransomware: This type of ransomware stays silent after infecting a device. The goal is to have it infect all backups. Then, when it's activated, the victim doesn't have a clean backup to restore.

Supply Chain Attacks: Supply chain attacks have been growing. They include attacks on cloud vendors that companies use. Those vendors suffer a cyberattack that then spreads throughout their clients.

Misconfiguration: Misconfiguration of security settings can be a problem. It can allow attackers to gain access to cloud storage. Those attackers can then download and delete files as they like.

WHAT TO LOOK FOR IN A DATA PROTECTION BACKUP SYSTEM

Just backing up data isn't enough. You need to make sure the application you use provides adequate data protection. Here are some of the things to look for when reviewing a backup solution.

***95%** of ransomware attacks also try to infect data backup systems.*

Ransomware Prevention

Ransomware can spread throughout a network to infect any data that exists. This includes data on computers, servers, and mobile devices. It also includes data in cloud platforms syncing with those devices.

It's important that any data backup solution you use have protection from ransomware. This type of feature restricts automated file changes that can happen to documents.

Continuous Data Protection

Continuous data protection is a feature that will back up files as users make changes. This differs from systems that back up on a schedule, such as once per day.

Continuous data protection ensures that the system captures the latest file changes. This mitigates data loss that can occur if a system crashes before the next backup. With the speed of data generation these days, losing a day's worth of data can be very costly.

Threat Identification

Data protection incorporates proactive measures to protect files. Threat identification is a type of malware and virus prevention tool. It looks for malware in new and existing backups. This helps stop sleeper ransomware and similar malware from infecting all backups.

Zero-Trust Tactics

Cybersecurity professionals around the world promote zero-trust security measures. This includes measures such as multi-factor authentication and application safelisting.

03 SOLVE IT SOLUTIONS, LLC, IS PROUD TO ANNOUNCE NEW MICROSOFT 365 CERTIFICATIONS EARNED BY ITS TEAM MEMBERS.

Solve IT Solutions, LLC, is proud to announce new Microsoft 365 certifications earned by its team members.

Preston Sleppy, Systems Engineer, after several months attending virtual sessions, has earned the Microsoft 365 Enterprise Administrator Expert Certification which includes accreditations in Microsoft 365 Security Administration, Microsoft 365 Identity and Services and Microsoft 365 Mobility and Security.

Individuals achieving these certifications carry expert-level skills in evaluating, planning, migrating, deploying and managing Microsoft 365. They can perform Microsoft 365 tenant-level planning, implementation and administration of cloud and hybrid enterprise environments and achieve expert-level knowledge of Microsoft 365 applications, infrastructure and identity.

Ulises Diaz, Technical Analyst, also completed virtual coursework to earn his Microsoft 365 Fundamentals Certification. Diaz demonstrated knowledge of the foundational-level of cloud services as well as a familiarity with current Microsoft 365 cloud offerings.

Preston, Ulises and the entire Solve IT Solutions Team take continuing education very seriously and are always eager to expand our knowledge to provide you with the best IT services.

Preston Sleppy

Ulises Diaz

04 WHY YOU NEED TO THINK TWICE BEFORE USING LENSA AI & OTHER SELF-PORTRAIT APPS

It's a common theme. You begin seeing these amazing CGI images of your friends on Facebook or Instagram. You think, "How can I make one?"

The latest of these modern vanity marvels to make the rounds is Lensa AI. You upload about 10 photos so the app can feed that data into its AI algorithm.

Then, once it maps your facial features, it generates several fantasy profile pics.

It sounds like a little harmless digital fun, right? That's what many companies making apps like this like you to think. Vanity is an easy sell.

But for Lensa AI and several similar self-portrait apps, you're paying more than you know. The cost comes from the data privacy rights you're giving up. And these can go far beyond the app itself.

WHY WORRY ABOUT DATA PRIVACY WITH LENSA AI & SIMILAR APPS?

Data Used to Track You
Once you download the Lensa AI app, it can track your phone activity in other apps.

Data Collected
By downloading Lensa AI, you permit it to track all kinds of data, including the purchases you make online.

Loss of Rights to Your Uploaded Images
Lensa AI Terms require you to grant a sub-licensable license to use, reproduce, modify, distribute, and create derivative works of your user content.

Get a Device Privacy Checkup
The more apps you use, the more complicated data privacy can get. Don't leave it to chance.

05

EVERY COMPANY IS NOW A TECHNOLOGY COMPANY

Whether you sell shoes or run an accounting firm, you need some type of technology to operate. Today's companies aren't just in the business of selling their own goods and services anymore. They also must master various types of digital tools.

- Technology is a Critical Part of Business
- Customers Expect an Excellent Digital Experience
- Employees Need Devices to Drive Productivity
- AI & Automation Help Companies Stay Competitive
- Information is Being Generated at a Rapid Pace
- Vendors/Suppliers are Leaving Legacy Systems Behind
- It's Difficult to Grow Without Tech Innovation
- Business Continuity Needs

06

6 STEPS TO EFFECTIVE VULNERABILITY MANAGEMENT FOR YOUR TECHNOLOGY

Technology vulnerabilities are an unfortunate side effect of innovation. When software companies push new updates, there are often weaknesses in the code. Hackers exploit these.

Software makers then address the vulnerabilities with a security patch. The cycle continues with each new software or hardware update.

61% of security vulnerabilities in corporate networks are over 5 years old.

Step 1 - Identify Your Assets

Step 2 - Perform a Vulnerability Assessment

Step 3 - Prioritize Vulnerabilities by Threat Level

Step 4 - Remediate Vulnerabilities

Step 5 - Document Activities

Step 6 - Schedule Your Next Vulnerability Assessment Scan

07

WINDOWS 8.1 JUST LOST ALL SUPPORT. HERE'S WHAT YOU NEED TO KNOW

The latest operating system to lose all support is Windows 8.1. Microsoft released the OS in 2013, and it was officially retired on January 10, 2023. Microsoft issued the following warning for companies:

"Continuing to use Windows 8.1 after January 10, 2023 may increase an organization's exposure to security risks or impact its ability to meet compliance obligations."

HERE ARE A FEW FACTS YOU SHOULD KNOW:

- The OS will still technically work.
- Your system will no longer receive security patches.
- Options for upgrading are Windows 10 or 11.

WHAT HAPPENS IF YOU DON'T UPGRADE?

- Security & Compliance Issues
- Slowed Productivity
- Incompatibility with Newer Tools