MAY 2023

Cirrus IT Services

TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

Why App Fatigue is a Security Issue ..... Page 1

Is your AntiVirus Solution Enough? ..... Page 1

Virtual Appointments in Microsoft Teams ..... Page 2

Everyday Objects Can Steal Your Identity ..... Page 2

Technologies to Give You an Advantage ..... Page 2

Tech Tip of the Month ..... Page 2

The Coolest Tech from CES ..... Page 2

Technology Trivia ..... Page 2

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing Technology!

- **Scott Magee**
Managing Director

WHAT IS APP FATIGUE & WHY IS IT A SECURITY ISSUE?

The number of apps and web tools that employees use on a regular basis continues to increase. Most departments have about 40-60 different digital tools that they use. 71% of employees feel they use so many apps that it makes work more complex.

Many of the apps that we use every day have various alerts. We get a "ping" when someone mentions our name on a Teams channel. We get a notification popup that an update is available. We get an alert of errors or security issues.

App fatigue is a very real thing and it's becoming a cybersecurity problem. The more people get overwhelmed by notifications, the more likely they are to ignore them.

Just think about the various digital alerts that you get. They come in:

- Software apps on your computer
- Web-based SaaS tools
- Websites where you've allowed alerts
- Mobile apps and tools
- Email banners
- Text messages
- Team communication tools

Some employees are getting the same notification on two different devices. This just adds to the problem.

This leads to many issues that impact productivity and cybersecurity.

Besides alert bombardment, every time the boss introduces a new app, that means a new password.

Employees are already juggling about 191 passwords.

They use at least 154 of them sometime during the month.

How Does App Fatigue Put Companies at Risk?

Employees Begin Ignoring Updates

When digital alerts interrupt your work, you can feel like you're always behind.

This leads to ignoring small tasks seen as not time-sensitive.

Tasks like clicking to install an app update.

Employees overwhelmed with too many app alerts, tend to ignore them.

When updates come up, they may quickly click them away. They feel they can't spare the time right now and aren't sure how long it will take.

Ignoring app updates on a device is dangerous.

Many of those updates include important security patches for found vulnerabilities.

When they're not installed, the device and its network are at a higher risk. It becomes easier to suffer a successful cyberattack.

Employees Reuse Passwords (and They're Often Weak)

Another security casualty of app fatigue is password security.

The more SaaS accounts someone must create, the more likely they are to reuse passwords. It's estimated that passwords are typically reused 64% of the time.

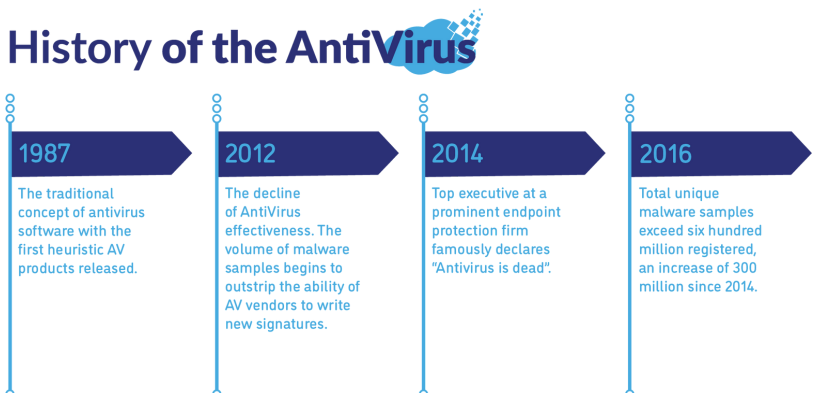
Credential breach is a key driver of cloud data breaches. Hackers can easily crack weak passwords. The same password used several times leaves many accounts at risk.

What's the Answer to App Fatigue?

It's not realistic to just go backward in time before all these apps were around.

But you can put a strategy in place that puts people in charge of their tech, and not the other way around.

- Streamline Your Business Applications
- Have Your IT Team Set up Notifications
- Automate Application Updates
- Open a Two-Way Communication About Alerts



Is your AntiVirus Solution Enough?

Did you know that today, the speed at which new viruses are unleashed outstrips the ability of most providers to write signatures, advanced state-sponsored attack techniques are becoming mainstream, and that the volume and complexity of malware has smothered EDR?

Our A.I. powered solution, SentinelOne, can stop even the most advanced attacks by analysing the behavioural data of applications, processes and network traffic. Find out more: ***cirrusits.co.uk/sentinelone-ai-antivirus/***

Cirrus IT Services

VIRTUAL APPOINTMENTS IN MICROSOFT TEAMS

In today's fast-paced world, the need for efficient and effective communication has never been more critical.

With the rise of remote work and the increasing reliance on technology, virtual appointments have become an essential tool for businesses and organizations worldwide.

Microsoft Teams, a powerful collaboration platform, has emerged as a game-changer in this arena, offering seamless virtual appointments that redefine the way we connect, collaborate, and communicate.

The Rise of Virtual Appointments

The global pandemic has accelerated the adoption of remote work, with businesses and organizations scrambling to find ways to maintain productivity and communication while keeping their employees safe.

Virtual appointments have become the go-to solution, allowing teams to connect and collaborate without the need for physical presence.

Microsoft Teams, a platform designed to facilitate teamwork and communication, has risen to the challenge, offering a comprehensive suite of tools that make virtual appointments a breeze.

From video conferencing to file sharing, Microsoft Teams has everything you need to conduct successful virtual appointments, all in one place.

Benefits of Virtual Appointments in Microsoft Teams

1. Enhanced Collaboration

Microsoft Teams allows users to collaborate in real-time, making it easier than ever to work together on projects, share ideas, and make decisions.

With features like screen sharing, whiteboarding, and file sharing, virtual appointments in Microsoft Teams enable teams to work together seamlessly, no matter where they are located.

2. Increased Flexibility

Virtual appointments in Microsoft Teams offer unparalleled flexibility, allowing team members to join meetings from any device, anywhere.

This means that employees can participate in important discussions and decision-making processes even if they're on the go or working from home.

3. Cost Savings

By eliminating the need for physical meeting spaces and reducing travel expenses, virtual appointments in Microsoft Teams can result in significant cost savings for businesses and organizations.

Additionally, the platform's robust features and integrations eliminate the need for multiple software subscriptions.

4. Improved Communication

Microsoft Teams' virtual appointments facilitate clear and effective communication, thanks to high-quality video and audio capabilities. The platform also offers features like live captions and translations, ensuring that language barriers and accessibility issues are no longer a hindrance to effective communication.

5. Enhanced Security

Microsoft Teams is built on the secure and reliable Microsoft 365 platform, ensuring that your virtual appointments are protected by enterprise-grade security measures. This means that you can conduct your meetings with confidence, knowing that your data and conversations are safe.

THESE EVERYDAY OBJECTS CAN LEAD TO IDENTITY THEFT

You wouldn't think a child's toy could lead to a breach of your personal data. But this happens all the time.

What about your trash can sitting outside? Is it a treasure trove for an identity thief?

Many everyday objects can lead to identity theft.

Old Smart Phones

A cybercriminal could easily strike data theft gold by finding an old smartphone. Make sure that you properly clean any old phones by erasing all data.

Wireless Printers

Protect wireless printers by ensuring you keep their firmware updated. You should also turn it off when you don't need it.

USB Sticks

You should never plug a USB device of unknown origin into your computer. This is an old trick in the hacker's book. They plant malware on these sticks and then leave them around as bait.

Old Hard Drives

When you are disposing of an old computer or old removable drive, make sure it's clean. Just deleting your files isn't enough.

It's best to get help from an IT professional to properly erase your computer drive. This will make it safe for disposal, donation, or reuse.

Trash Can

Identity theft criminals aren't only online. They can also be trolling the neighborhood on trash day. Be careful what you throw out in your trash.

Children's IoT Devices

You should be wary of any new internet-connected kids' devices you bring into your home. Install all firmware updates and do your homework.

ATMs

This is called skimming. Malicious actors can use hidden devices on ATMs or card readers to steal your card information during transactions.

TECHNOLOGIES TO GIVE YOU AN ADVANTAGE

Customers look for convenience. In today's world that means technology that makes their life easier.

From webforms to POS systems, you need to keep the customer experience in mind in all you do.

When people aren't happy with their experience interacting with a company, they leave.

And their experience might not have anything to do with your products or services. Maybe they found it hard to navigate your website.

Technology is key to converting website visitors into clients.

These techonologies can give you that edge:

- Cloud Forms
- Digital Signatures
- Smart Chatbot
- SMS Notifications
- Business Mobile App
- FAQ Kiosk
- VoIP Phone System

6 THINGS YOU SHOULD DO TO HANDLE DATA PRIVACY UPDATES

Once data began going digital, authorities realized a need to protect it. Many organizations have one or more data privacy policies they need to meet.

Industry and international data privacy regulations are just the tip of the iceberg. Here are a few things you should look into to handle data privacy updates:

1. Identify the Regulations You Need to Follow
2. Stay Aware of Data Privacy Regulation Updates
3. Do an Annual Review of Your Data Security Standards
4. Audit Your Security Policies and Procedures
5. Update Your Technical, Physical & Administrative Safeguards As Needed
6. Keep Employees Trained on Compliance and Data Privacy

SINGLE-SIGN-ON MADE EASY WITH JUMPCLOUD SSO

Quickly accessing your apps at work shouldn't feel like a chore for employees.

90% of respondents to business solution firm Freshworks' survey about tech at work said that they are often frustrated with their experience using computers and software.

This leads to employee burnout and brings down the business' productivity.

With JumpCloud, you can use one set of credentials to access your PC, Microsoft 365 (your Outlook, Word and Excel) and other services such as Adobe.

Here are some of the key features to consider:

- Ease of access to applications and services
- Reduce password & MFA fatigue
- Control devices and user accounts through built-in policies
- Increase compliance management abilities
- Revoke & Grant access to users with ease

To find out more contact us today at info@cirrusits.co.uk, or visit:

cirrusits.co.uk/jumpcloud-sso

TECHNOLOGY TRIVIA TIME

Each month you have a chance to win an Amazon Gift Card! Our April competition winner (randomly selected from correct entries) was:
Hannah Kibble!

Congratulations, Hannah!

The question this month is:

What material was the first computer mouse made of?

Email us at hello@cirrusits.co.uk with the correct answer by 15th May 2023 for your chance to win! Good Luck!