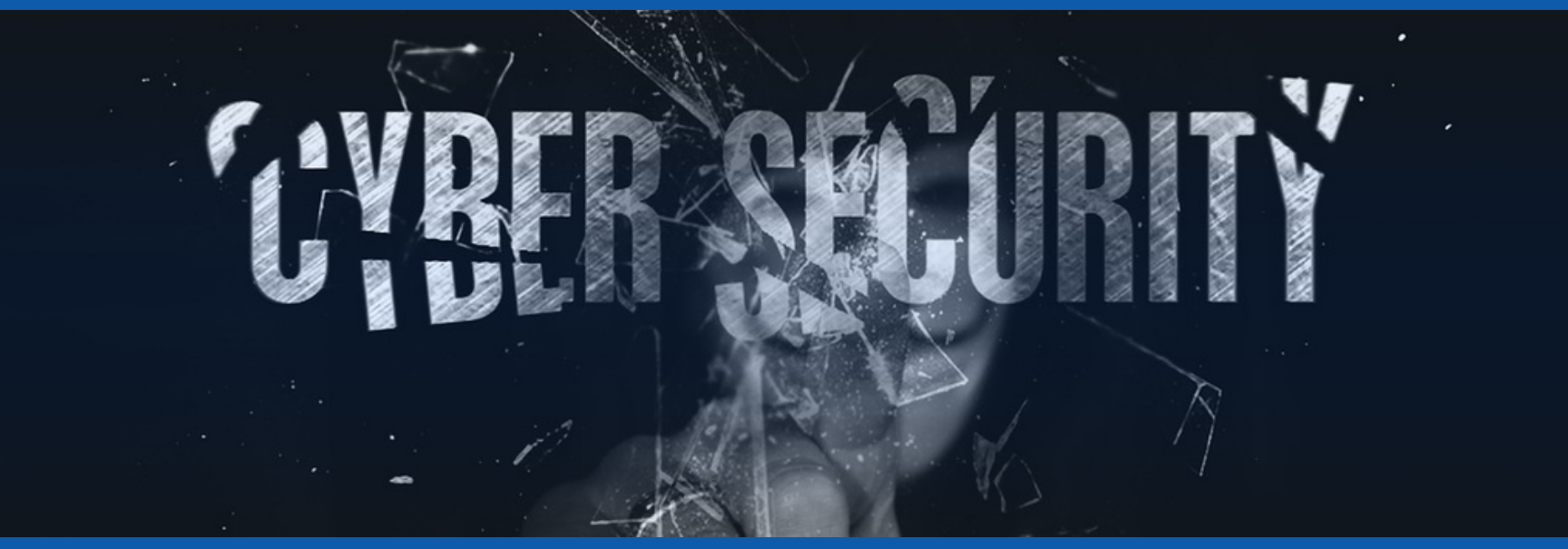
ESP PROJECTS LTD
OCTOBER 2023



TECH TALK

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

INSIDE THIS ISSUE:

"Cybersecurity Skeletons" in the Closet	Page 1	9 Reasons to Use Airplane Mode	Page 2
#ESPDuck - Missy	Page 1	Tech Tip of the Month	Page 2
What is SaaS Ransomware?	Page 2	Learning Essential Cyber Hygiene	Page 2
The New Microsoft Intune Suite	Page 2	Events and Training	Page 2

We love technology and we love helping people. Welcome to Autumn, as the seasons change and a new School year begins its a good time to review your IT and Security. Give me a call today 0330 2020 101 for a quick chat to find out more.

Donna Aplin

Marketing Manager

CYBERSECURITY SKELETONS IN YOUR BUSINESS' CLOSET

Let's dive into a topic that might give you the chills—cybersecurity skeletons in the closet. You may not have old skeletons hidden away in the basement, but there's a good chance of cybersecurity vulnerabilities lurking in the shadows. Just waiting to wreak havoc.

You can't fix what you can't see. It's time to shine a light on these hidden dangers, so you can take action to protect your business from potential cyber threats.

Here are some of the most common cybersecurity issues faced by SMBs:

Outdated Software: The Cobweb-Covered Nightmare

Running outdated software is like inviting hackers to your virtual Halloween party.

When software vendors release updates, they often include crucial security patches. These patches fix vulnerabilities that hackers can exploit. Keep everything up to date to ensure your digital fortress is secure.

Weak Passwords: The Skeleton Key for Cybercriminals

If your passwords are weak, you might as well be handing out your office keys to cybercriminals.

Instead, create strong and unique passwords for all accounts and devices. Consider using a mix of upper and lowercase letters, numbers, and special characters.

Unsecured Wi-Fi: The Ghostly Gateway

Ensure your Wi-Fi is password-protected. Make sure your router uses WPA2 or WPA3 encryption for an added layer of security. For critical business tasks consider a virtual private network (VPN). It can shield your data from prying eyes.

Lack of Employee Training: The Haunting Ignorance

Employee error is the cause of approximately 88% of all data breaches.

Without proper cybersecurity training, your staff might unknowingly fall victim to phishing scams. Or inadvertently expose sensitive information. Regularly educate your team about cybersecurity best practices.

Such as:

- Recognising phishing emails
- Avoiding suspicious websites
- Using secure file-sharing methods

No Data Backups: The Cryptic Catastrophe

Imagine waking up to find your business's data gone, vanished into the digital abyss. Without backups, this nightmare can become a reality.

Embrace the 3-2-1 rule. Have at least three copies of your data, stored on two different media types. With one copy stored securely offsite.

No Multi-Factor Authentication (MFA): The Ghoulish Gamble

Adding MFA provides an extra layer of protection. It requires users to provide extra authentication factors. Such as a one-time code or passkey. This makes it much harder for cyber attackers to breach your accounts.

Disregarding Mobile Security: The Haunted Phones

Ensure that all company-issued devices have passcodes or biometric locks enabled. Consider implementing mobile device management (MDM) solutions. These will enable you to enforce security policies.

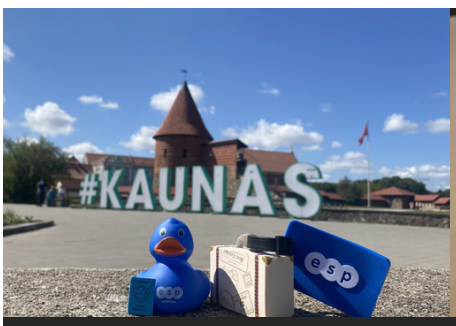
Shadow IT: The Spooky Surprise

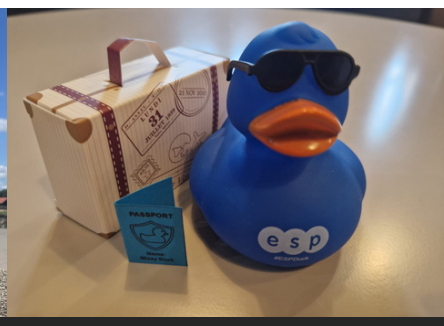
Shadow IT refers to the use of unauthorised applications within your business. It might seem harmless when employees use convenient tools they find online.

Regularly audit your systems to uncover any shadow IT lurking under cover.

Incident Response Plan: The Horror Unleashed

Develop a comprehensive incident response plan. It should outline key items such as how your team will detect, respond to, and recover from security incidents. Regularly test and update the plan to ensure its effectiveness.





Missy's #ESPDuck - Summer World Tour.....

Missy has been well and truly on her travels this summer - thank you to all of you that have sent in pictures of her on her visits to many places in the world. She has been far and wide taking in sites from Italy, Lithuania, Spain, Greece, Morocco, Australia, Ireland, USA, lots of UK destinations....

The list goes on! We held a competition over the summer for the best picture from Missy's travels and the winner was announced on our socials at the end of September as Indre Pociute from Ares Landscape Architects Ltd - Congratulations we will be in touch!!

WHAT IS SAAS RANSOMWARE? HOW CAN YOU DEFEND AGAINST IT?

Software-as-a-Service (SaaS) has revolutionised the way businesses operate. But alongside its benefits, SaaS brings with it potential threats. When software and data are online, they're more vulnerable to attacks. One of the latest threats to move from endpoint devices to the cloud is ransomware.

Between March and May of 2023, SaaS attacks increased by over 300%. A study in 2022 by Odaseva found that 51% of ransomware attacks targeted SaaS data.

What is SaaS Ransomware?

SaaS ransomware is also known as cloud ransomware. It's malicious code designed to target cloud-based applications and services. These include services like Google Workspace, Microsoft 365, and other cloud collaboration platforms.

Defending Against SaaS Ransomware

Educate Your Team

Start by educating your employees about the risks of SaaS ransomware. Include how it spreads through phishing emails, malicious links, or breached accounts. Teach them to recognise suspicious activities and report any unusual incidents immediately.

Enable Multi-Factor Authentication (MFA)

MFA is an essential layer of security. Enabling MFA reduces the risk of unauthorised access. This is true, even if a hacker compromises an account's login credentials.

Regular Backups

Frequently backing up your SaaS data is crucial. Having up-to-date backups ensures that you can restore your files. You won't need to pay the attacker's ransom demands.

Apply the Principle of Least Privilege

Limit user permissions to only the necessary functions. By doing this, you reduce the potential damage an attacker can do if they gain access.

Keep Software Up to Date

Ensure that you keep all software up to date. Regular updates close known vulnerabilities and strengthen your defense.

Deploy Advanced Security Solutions

Consider using third-party security solutions that specialise in protecting SaaS environments. These solutions can provide many benefits. Including:

- Real-time threat detection
- Data loss prevention
- And other advanced security features

Track Account Activity

Put in place robust monitoring of user activity and network traffic. Suspicious behavior can be early indicators of an attack. One example to watch for is several failed login attempts. Another is access from unusual locations.

Develop an Incident Response Plan

Prepare and practice an incident response plan. It should outline the steps to take in the event of a ransomware attack. A well-coordinated response can mitigate the impact of an incident. It can also aid in faster recovery. The sooner your team can respond, the faster business gets back to normal.

SHOULD YOUR BUSINESS UPGRADE TO THE NEW MICROSOFT INTUNE SUITE?

Endpoint management has changed a lot over the last two decades.

The average enterprise endpoint makeup is 60% mobile devices. And it's estimated that they handle about 80% of the workload. What does this mean for security? That's why an endpoint device management solution has become a necessity.

One that might be on your radar is the new Microsoft Intune Suite. It bundles several areas of endpoint management into a single platform.

What Does Microsoft Intune Suite Include?

It includes all the core features of Intune, plus:

- Microsoft Intune Remote Help
- Microsoft Intune Endpoint
- Privilege Management
- Microsoft Tunnel for Mobile
- Application Management
- Management of specialty devices
- Select Microsoft Intune advanced endpoint analytics features

Advantages of Subscribing

- Streamlined Device Management
- Provide Secure Helpdesk Support
- Enhanced Security and Compliance
- App Management Made Easy
- BYOD-Friendly
- Scalability and Cost-Effectiveness

What Do You Need to Consider?

Alright, those are some pretty compelling reasons to consider Microsoft Intune Suite. But let's take a moment to address some potential downsides you need to consider as well.

Learning Curve

One common concern is the learning curve. Luckily, we can help you with training and support to ensure a smooth shift.

Do You Have Legacy Systems?

Does your business rely on legacy systems or run a large number of onpremises servers? Then integrating Intune into your existing setup may take some extra effort.

9 REASONS TO USE AIRPLANE MODE EVEN IF YOU'RE NOT TRAVELING

Most people are familiar with their device's Airplane Mode. You've probably used it when jetting off to exotic locations. But did you know that it's not just for globetrotters?

That's right! Airplane Mode isn't only for flying; it can be a handy feature for your everyday life.

Here are some top reasons why you should consider toggling it on, even if you're not traveling.

1. Save that precious battery life
2. Boost your charging speed (by about 4x)
3. A tranquil escape from notifications
4. Focus Mode: Engaged!
5. Prevent embarrassing moments
6. Roaming woes, be gone!
7. A digital detox
8. Avoid unwanted radiation
9. Save data and money

TIPS TO OPTIMISE A DUALMONITOR SETUP

Two monitors are often better than one when it comes to getting things done efficiently. A dual-monitor setup can significantly enhance your productivity. This is true whether you're a gamer, a creative professional, or an office wiz who loves to multitask.

It's common for people to feel "off kilter" when trying to work from two monitors. The cause is usually the setup.

Here are some dual-monitor setup best practices to help you improve your two-screen experience and take it to the next level.

1. Match size and resolution
2. Get the right cables
3. Positioning is everything
4. Embrace the Extended Desktop
5. Focus on Taskbar Tweaks
6. Leverage Shortcuts
7. Gaming in style

LEARNING ESSENTIAL CYBER HYGIENE

As technology continues to advance, so does the need for heightened awareness. As well as proactive measures to safeguard sensitive information.

Cybersecurity can seem like an insurmountable task for everyday people. But it's not only a job for the IT team. Everyone can play a part in keeping their organisation's data safe. Not to mention their own data.

October is Cybersecurity Awareness Month.
It serves as a timely reminder that there are many ways to safeguard data. Following the basics can make a big difference in how secure your network remains.

This is CAM's 20th year. To celebrate, the theme revolves around looking at how far cybersecurity has come. As well as how far it has to go. This year, CAM focuses on four key best practices of cybersecurity:

- Enabling multi-factor authentication
- Using strong passwords and a password manager
- Updating software
- Recognising and reporting phishing

Events and Training

September was a busy month here at ESP Projects, we hosted the third event in our series - this covered Business Backup and Future Proofing your Business. We have also hosted 2 training sessions for staff members within a business on the theme of educating and upskilling your staff on using Microsoft 365. If you would like more information on these sessions contact us on 0330 2020 101 or send a an email to marketing@espprojects.co.uk.