FROM DAMIEN'S DESK:

TIK TOK. Who would have thought this seemingly harmless APP would have caused such an uproar? In most people's minds, it is just sharing short videos with a global audience. Some might say, like YouTube.

Well, it has been proven that this is not the case. While it does its intended function well, it also records a lot of personal data with each recorded video and potentially shares that information with the TIK TOK servers. The TIK TOK app collects data from your phone, **even when you are not using the app.**

It has been alleged that it collects items like your connection's IP address, the phone's GEO location, your contacts and even which direction you are facing. The underlying owner of TIK TOK is Byte Dance, a Chinese technology company.

Our government has raised concerns about the Chinese government potentially mandating Byte Dance to hand over all data stored on our citizens. We will see more on this in the coming weeks and months.

Remember, one level of security for your business should be the appropriateness of using apps and programs on company equipment or within the company network.

I urge you to consider whether TIK TOK is really an appropriate app for your company devices or to be used in your company network.

Stay safe out there

Damien Pepper - Managing Director
dsp IT Solutions

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.

For your FREE copy of this book, go to:
https://www.dspit.com.au/cybersecurity-essentials/

dsp IT Solutions
182C Sladen Street
Cranbourne VIC 3977
(03) 9001 0817
sales@dspit.com.au
www.dspit.com.au

#SuperResponsive #WeMakeTheComplexSimple #BuildRelationships #NothingIsTooHard

APP FATIGUE IS A THING! HERE'S HOW TO FIGHT IT

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:
- 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 Organisations 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.

cont'd P3

cont'd from P2

Employees May Turn Off Alerts

Some alerts are okay to turn off. For example, do you really need to know every time someone responds to a group thread?

But, turning off important security alerts is not good.

There comes a breaking point when one more push notification can push someone over the edge.

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

4 PROVEN WAYS TO MITIGATE THE COSTS OF A DATA BREACH

No business wants to suffer a data breach. But unfortunately, in today's environment, it's difficult to completely avoid them. Approximately 83% of organisations have experienced more than one data breach.

(IBM Security 2022: https://www.ibm.com/reports/ data-breach)

The global average cost of a data breach is now $4.35 million, up 2.6% from last year.

Companies don't need to resign themselves to the impending doom of a breach. There are some proven tactics they can take to mitigate the costs.

1. Use a Hybrid Cloud Approach

Breaches in both the public cloud and private cloud cost more than those in organisations using a hybrid cloud approach.

2. Put in Place an Incident Response Plan & Practice It

Having a practiced incident response plan reduces the cost of a data breach. It lowers it by an average of $2.66 million per incident.

3. Adopt a Zero Trust Security Approach

Organisations that don't deploy zero trust tactics pay about $1 million more per data breach.

4. Use Tools with Security AI & Automation

Data breach expenses lower by 65.2% thanks to security A.I. and automation solutions. These types of solutions include tools like Advanced Threat Protection (ATP).

Need Help Improving Your Security & Reducing Risk?

Working with a trusted IT partner takes a lot of the security burden off your shoulders. Give us a call today to schedule a chat about your Cybersecurity.

6 THINGS YOU SHOULD DO TO HANDLE DATA PRIVACY UPDATES

Once data began going digital, authorities realised a need to protect it. Many organisations 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:

- Identify the Regulations You Need to Follow
- Stay Aware of Data Privacy Regulation Updates
- Do an Annual Review of Your Data Security Standards
- Audit Your Security Policies and Procedures
- Update Your Technical, Physical & Administrative Safeguards as Needed
- Keep Employees Trained on Compliance and Data Privacy

EVERY ORGANISATION IS NOW A TECHNOLOGY ORGANISATION

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

The following points are good to keep in mind when it comes to technology and your organisation:

- 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

WE LOVE REFERRALS . .

The greatest gift anyone can give us is a referral to your business colleagues/ friends. Referrals help us keep costs down so we can pass the savings on to our clients. Simply introduce me via email to damien@dspit.com.au or (03) 9001 0817 and I'll take it from there.

NEED A LAUGH?

What shoes do computers love the most?

Re-boots!

WIN A $20 BUNNINGS GIFT CARD!

There was no winner for last month's trivia question. The answer was c) LasVegas.com

You could be the winner of this month's trivia question.
Just contact us with the answer to the question below, Good Luck!

What did Nokia originally sell/make?

a) They were a paper manufacturer in 1865
b) They sold handset phones in 1985
c) They have only ever sold/made mobile phones
d) They sold greeting cards in 1920

Call us with your answer (03) 9001 0817 or email jo@dspit.com.au