PGI Cyber Bytes

Your monthly cyber snapshot

15th May 2018

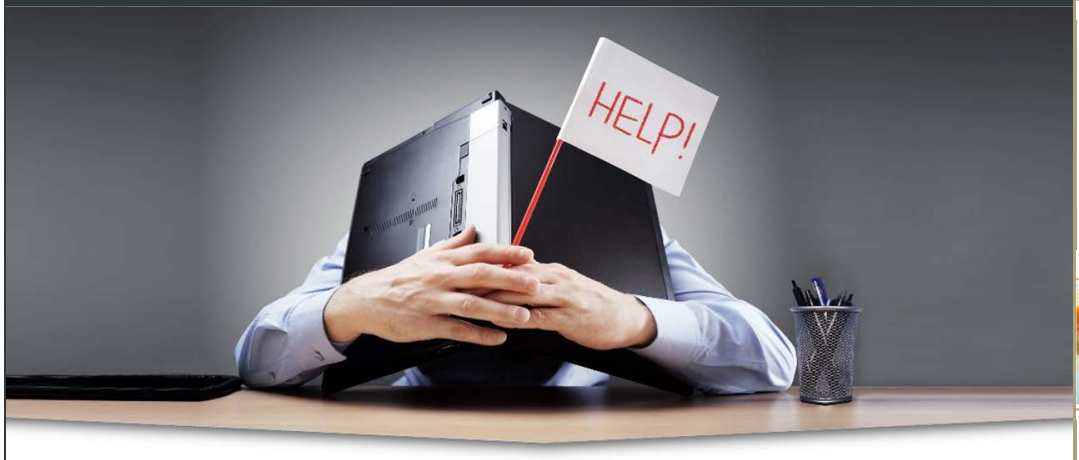
Visit Our Website

Can't read this email properly?

We hope you have been enjoying our Cyber Bytes series.

Keep an eye on our social media channels for ongoing news from the world of information security and PGI.

Humans Are Still the Weakest Link



A recent survey of decision makers from IT, risk, fraud and compliance departments at various UK companies have found that almost 70% of successful ransomware attacks last year were the result of hackers gaining access via phishing emails or social media phishing campaigns.

Public awareness of the threat of ransomware has certainly increased following several high profile ransomware attacks, such as WannaCry and NotPetya, but this latest research from security software company SentinelOne demonstrates that many people are still failing to identify malicious phishing emails.

The advice to any victims remains that ransom demands should not be paid, but the research also found that victims actually paid an average of £34,845 to recover their files after an attack.

Hyperlink Tip

Be careful about clicking on links without revealing the destination first. You can hover over the links in this e-mail to reveal the URL so you know where it is taking you to, prior to clicking.

Phishing – How Vulnerable is your Workforce?

We have mentioned Phishing a lot in this month's Cyber Bytes. A whopping 90% of breaches involve phishing, and your workforce is a hacker's number one entry port.

With a little training and some vulnerability assessments your risk can be massively reduced.

Perhaps more concerning is that 58% of the respondents admitted that even though their organisation had paid the ransom, the perpetrators then tried to extort a second payment and 42% said their files were not decrypted even though they had met the ransom demands.

PGI offer a Phishing Vulnerability Assessment. We will send a series of mock malicious e-mails to your staff to gauge their vulnerability to compromised links, followed by training.

Read the full PGI article here

Victims Ahoy! Gold Galleon Crew Sets Course for Shipping Execs

Researchers from the Secureworks Counter Threat Unit (CTU) have recently uncovered a threat group known as Gold Galleon, who have been targeting victims via Business Email Compromise (BEC).

BEC is a targeted phishing technique where criminals attempt to gain access to business email accounts, typically those of Financial Directors or finance/account executives, which enables them to intercept the emails and transactions between two companies. At an appropriate time, they then modify the financial details of transactions to direct funds to their own accounts. What makes the Gold Galleon crew unique amongst other BEC groups is that they appear to be focussing their attacks solely on global maritime shipping businesses and their customers.

Read the full PGI article here

Researchers Show How Amazon Echo Can be Used for Eavesdropping

PGI can conduct a series of mock malicious e-mails to your staff, based on open source knowledge of your organisation, followed by a vulnerability report and training.

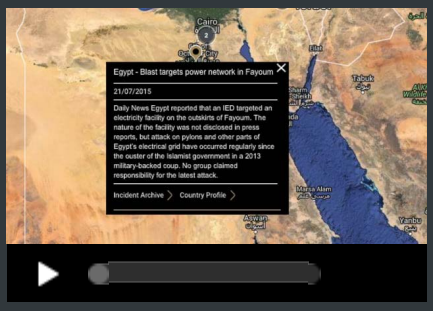
Interested? Visit our webpage, download our datasheet or contact us directly.

Starting at £499 for basic assessments.

Find out more

The PGI Risk Portal

Your global geopolitical risk dashboard.



PGI's Risk Portal tool provides daily intelligence feeds, country threat assessments and analytical insights, enabling clients to track, understand and navigate geopolitical threats.

Click here to sign up

"Privacy became a top-of-mind issue with the introduction of personal assistants like the Siri-enabled Apple HomePod, Google Home and Amazon's Alexa-powered Echo. Many believed these products could be used as tapping devices.

Turns out they were right, as evidenced by two researchers who fed malware to Amazon's Echo and turned it into a "bug."

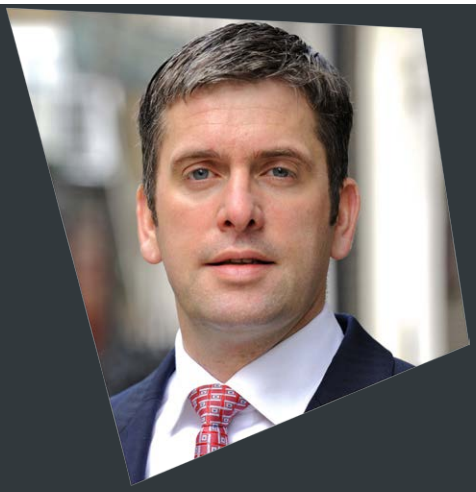
Although technically always on, voice-enabled assistants stream information to and from the cloud only after a key wake-up signal – in the case of Echo, calling out the name of the AI persona that does the talking: Alexa…."

PGI says...

This is not a new problem. As the article intimates, Siri enabled devices like iPhones, as well as similar listening services like Cortana, have been around for several years. These have been quietly listening to everything around them waiting for their wake up call too. Many people find the services these assistants provide to be very helpful.

There is a catch though: any device which is connected to the internet is at risk of being compromised. As well as being able to listen and wait to be woken up, the device could be configured to stream everything that is being said, as well as other ambient sounds.

Why is this a risk? Imagine that you're talking about your upcoming holiday: whoever is listening at the other end now knows when you'll be gone, for how long, where you're travelling



Barry's Bytes

Recommendations from our CEO and other PGI employees

For the readers

This weeks recommendation is a follow up to The Talent Code, and focuses in a similar way with culture.

The Culture Code: The Secrets of Highly Successful Groups
by Daniel Coyle

It gives some interesting insights into creating highly effective teams and it will be very different to what you might think.

For the watchers

to and from etc. This could give them plenty of time to break in to your house.

Alternatively, what happens if you're talking in a meeting room, discussing plans for a merger / acquisition, and your competitors find out what your plans are, how much you're willing to spend etc. This could lead to a serious competitive advantage for them.

PGI's advice would be to ensure that any software updates are applied as soon as possible, and that you exercise caution around what is said within listening range of these devices.

Read the full source article here

PGI in Pictures

Last week we launched our 'Cyber Retraining Programme' here at the Academy in Bristol. We are training candidates with little or no experience and knowledge within information security, so they are skilled enough to walk into paid jobs following the programme.

The candidates are understandably excited, with one noting 'this will completely change my career, I can't wait'.

Click the icon for the YouTube link.

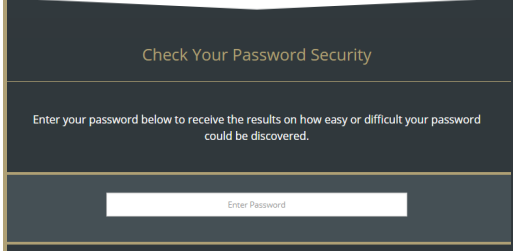
Forward to a Friend

We want to keep as many people as possible up to date with industry news. Please feel free to forward this e-mail to any of your friends and colleagues.

Even better, why don't they

Subscribe here

by completing our message box.



Check Your Password Security.

This online service allows you to evaluate the strength of your password.

You can use this checker to see how length and characters such as !&@ all help to make your password more secure from malicious hackers.

Click here to check your password

Follow us:

Phone: +44 (0) 207 887 2699
Email: clientservices@pgitl.com
Visit our site

PGI Cyber Academy
Cascades 1 | 1190 Park Avenue Aztec West | Bristol | BS32 4FP | UK