



 **Croner-i**
Inform • Advise • Protect

AIB2021
virtual


Cyber risk in the new hybrid working environment


Dr Stephen Hill

1

Introduction

- Every organisation is responsible for ensuring cybersecurity
- The ability to protect information systems from impairment or even theft is essential
- Implementing effective security measures will not only offer liability protection; it will also increase efficiency and productivity...



 **Croner-i**
Inform • Advise • Protect

AIB2021
virtual

Dr Stephen Hill


2


Cyber Risk

*Cyber risk is not just an IT risk, it is an enterprise, strategic, commercial, and **organisation-wide** risk*

Cyber risk could include:

Cyber threats, social media, mobile devices, massive data storage, artificially intelligent products, the Internet of Things (IoT), privacy requirements, and continuity of business-as-usual and more...




 **AIB2021**
Inform • Advise • Protect virtual

Dr Stephen Hill

3


Quote for the Day



“One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks.

Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats”

Stephane Nappo
Global Head Information Security Société Générale

 **AIB2021**
Inform • Advise • Protect virtual

Dr Stephen Hill

4





What are the biggest cyber threats facing you and your business today?


Croner-i Inform • Advise • Protect **AIB2021** virtual

5

Alarming Rise in Pandemic-Related Cybercrime

- 

67% of IT leaders predict an increase in targeted phishing emails in which cybercriminals take advantage of the transition back to working in the office
- 

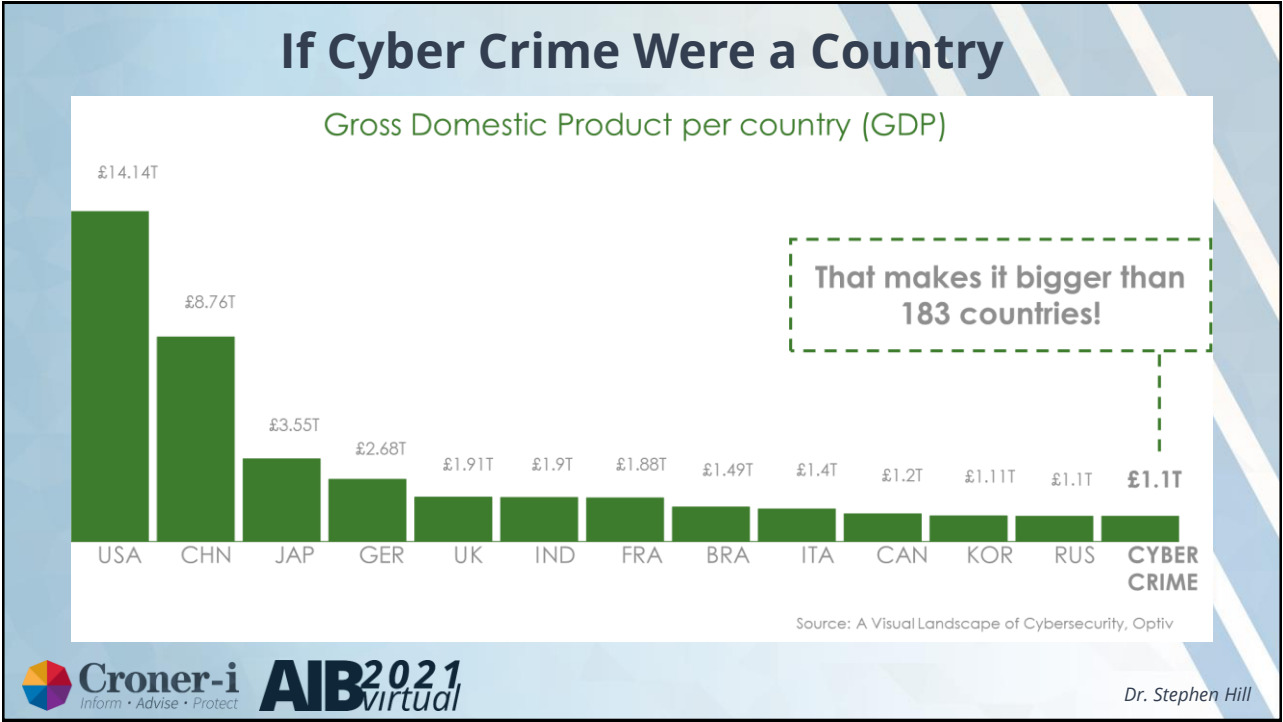
Microsoft reports that pandemic-themed phishing and social engineering attacks have jumped by **10,000 a day**
- 

Cyber security experts report that ransomware attacks are up by **800%**

Source: MonsterCloud, Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic

Croner-i Inform • Advise • Protect **AIB2021** virtual Dr Stephen Hill

6



7



8

Why Should I Care About Cybercrime?

Victims of cyber attacks experience a variety of losses:



CUSTOMER PROTECTION



COMPANY REPUTATION



CAREER DAMAGE



FINANCIAL COST



PRODUCT PROTECTION

Capital One shares dive after data breach affecting 100 million

Reputational Damage

KEY POINTS

- Capital One says it discovered the breach on July 19, adding the Social Security numbers of about 140,000 credit card customers were compromised, along with 80,000 bank account numbers.
- The breach also exposed names, addresses, phone numbers and credit scores, among other data.
- "This headline is not good one for Capital One," says RBC Capital Markets analyst Jon Arfstrom. "We worry about longer term reputational damage and also the potential for political and regulatory actions, including penalties."

What to Expect in 2021/2?

- The cloud will remain a top target
 - Hackers constantly target opportunistic gaps in a cloud platforms' security structures
- Ransomware incidents are predicted to get worse
 - Attacks will be targeted towards individuals, schools, hospitals, and small businesses as opposed to large corporations
- Weaponised AI
 - Hackers can use AI to develop constantly mutating malware that can mimic legitimate programs to avoid detection
- The implementation of 5G
 - Higher speeds mean faster attacks...

Key Reasons Cyber Attacks Are Possible



1. Optimism Bias: "It won't happen to me"
2. Passwords: Still too easy to crack
3. Software updates: "We push them to the back burner"
4. Email Complacency: Spotting a fake is NOT obvious
5. Lack of basic network security protection (not using two factor authentication)...

A PERPETRATOR'S STORY

MAKSIM VIKTOROVICH YAKUBETS

WANTED BY THE FBI
MAKSIM VIKTOROVICH YAKUBETS
 Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	Place of Birth: Ukraine
Date(s) of Birth Used: May 20, 1987	Eyes: Brown
Hair: Brown	Weight: Approximately 170 pounds
Height: Approximately 5'10"	Race: White
Sex: Male	
Citizenship: Russian	

REWARD
 The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to \$5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

'Cybercriminals are recruited to Russia's national cause through a mix of coercion, payments, and appeals to patriotic sentiment,' reads a 2017 story from The Register about security firm Cybereason's analysis of the Russian cybercrime scene.

'Russia's use of private contractors also has other benefits in helping to decrease overall operational costs, mitigate the risk of detection, and gain technical expertise that they cannot recruit directly into the government. Combining a cyber-militia with official state-sponsored hacking teams has created the most technically advanced and bold cybercriminal community in the world.'

Source: The Register, "Russia is struggling to keep its cybercrime groups on a tight leash," June 2017

Dr Stephen Hill

A Victims Story

PETHA ransomware

Start Payment FAQ Support English

Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

The price will be doubled in:

6 days, 13 hours, 43 minutes, 10 seconds

Start the decryption process

Dr Stephen Hill



15



16

Facebook is the latest major tech company to let people work from home forever

The social media giant is letting its employees request to permanently work from home.

By **Shirin Ghaffary** | May 21, 2020, 4:41pm EDT

f SHARE



Munich Security Conference **msc**
Münchner Sicherheitskonferenz

ESCHER HOF

urity nce **mso**
chernetskonferenz

BAYERISCHER HOF

THE LATEST



The real stakes of Apple's battle over remote work



Croner-i **AIB2021**
Inform • Advise • Protect *virtual*

17

REMOTE WORK & CYBER SECURITY

36% of organisations have dealt with a security incident due to an unsecured remote worker.

With the rise in hybrid and remote work, IT security focus has shifted from the perimeter, network, and firewalls to endpoints, end users, and email as the first line of remote defence.



ENDPOINTS

54% of IT decision makers are worried remote workers will bring infected devices and malware into the office.



EMAIL

Since the onset of the pandemic, employees are clicking on **3x** as many malicious emails as they were before.



END USERS

86% of UK businesses haven't had training or awareness sessions on cyber security in the last 12 months, as of early 2021.

Croner-i **AIB2021**
Inform • Advise • Protect *virtual*

Sources: OpenVPN, Tessian, Mimecast, National Cyber Security Centre

Dr. Stephen Hill

18



Working remotely

INFOSEC

Working remotely is safer, right?
Working remotely means you may be working with a home setup you can control, but if you're working from someone else's Wi-Fi, it may not be secured. Physical security is a concern without the protection of the secured office.

So I need a strong Wi-Fi password, right?
Definitely! But not just that. Your router has a separate password, one that you may never have changed. Make sure your router and Wi-Fi passwords are both strong and unique.

My router, too? Is there anything else that needs a password?
Phones, tablets and smart devices all need strong passwords, it's especially important with smart devices, which often come with default passwords that are forgotten or ignored, just like routers.

This sounds like a lot of trouble. Can I just use someone else's Wi-Fi?
It's not a good idea to work remotely over someone else's network. You don't know what protections (if any) that person or business has set up. Despite this, a survey found that 81% of people still connect to unsecured public networks.

What about the home office itself?
Setting up a home office means you're in charge of physical and digital security. It's important to invest in antivirus, shred unneeded documents ASAP, follow your organization's security policies to the letter and make sure that family members and friends don't use your work computer.

What's one thing I can do to improve my remote security?
Set up a VPN. A VPN or Virtual Private Network, establishes a secure encrypted connection, tunnelling data directly from the host to its destination. This is a great way to protect information when it's travelling across an insecure network.

- Be safer with strong passwords
- Know what needs to be protected
- Using public Wi-Fi – warning!
- Ramp up your security awareness
- Guard your login credentials
- Use a VPN
- Be smart and ratchet up your security outlook...



Croner-i
Inform • Advise • Protect


AIB²⁰²¹
virtual

Dr. Stephen Hill

19

The Challenge

- Remote work is a real challenge for information security because this kind of work environment doesn't typically have the same safeguards as in the office
- Performing in the office, employees follow the layers of preventive security controls
- When their computers leave the office and individuals work from home, new risks arise, and additional security policies seem essential...



Croner-i
Inform • Advise • Protect

AIB²⁰²¹
virtual

Dr. Stephen Hill

20

HR Tech | Legal | HR Strategy | Engagement & Performance

'Ticking time bomb' | Frustrated home workers in danger of causing IT 'security crisis'

Mon, 13 Sep 2021 | News | Kieran Howells | 3 mins read



Stringent security measures were an immediate concern in the move to home working, as gaining access to sensitive information and work-based discussions progressed remotely. However, new data from HP has found that younger workers are growing frustrated over accessibility.


<https://www.hrgrapevine.com>

Croner-i Inform · Advise · Protect **AIB2021** virtual


Dr Stephen Hill

21

Working from Home Do's & Don'ts Guide



<https://www.globalsign.com/en/blog/infographic-remote-work-and-security-7-dos-and-donts>



Croner-i Inform · Advise · Protect **AIB2021** virtual

Dr Stephen Hill

22

As we return to work just be cautious of existing and new scams that affect us on the move!



 **Croner-i**
Inform • Advise • Protect

AIB2021
virtual

Dr Stephen Hill

23



 **Croner-i**
Inform • Advise • Protect

AIB2021
virtual

24

Stop! Don't Charge Your Phone This Way

You might want to think twice before plugging in at an airport or on the train.



Juice jacking happens when unsuspecting users plug their electronic devices into USB ports or use USB cables that have been loaded with malware.

The malware then infects the devices, giving hackers a way in. They can then read and export your data, including your passwords, and even lock up the gadgets, making them unusable.

Juice jacking exploits the fact that somebody doesn't have a full battery, said Liviu Arsene, a cyber security expert at BitDefender, a Romanian cybersecurity and antivirus software company.




Dr Stephen Hill


25

Charge Safely

Protect your mobile phone from accidental syncing and malware!



View Video









Protect your data

SyncStop prevents accidental data exchange when your device is plugged into someone else's computer or a public charging station. SyncStop achieves this by blocking the data pins on any USB cable and allowing only power to flow through. This minimizes opportunities to steal your data or install malware on your mobile device.

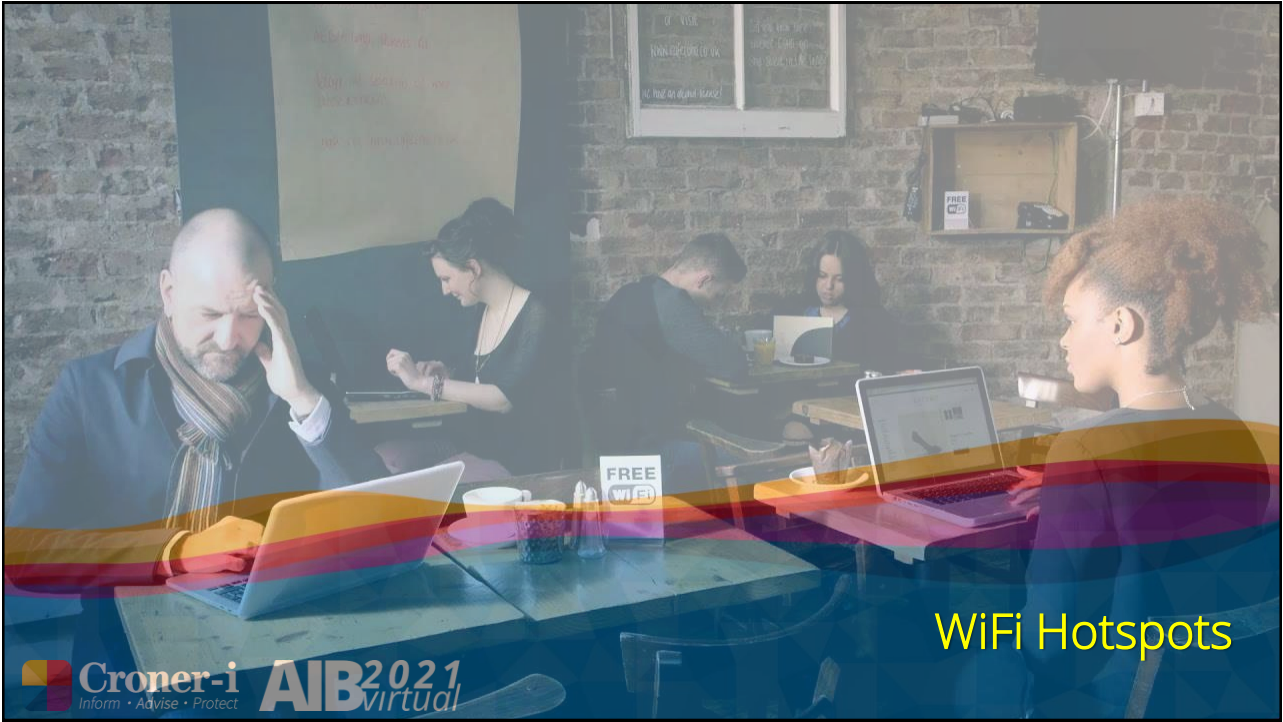
SyncStop is the 'cased' version of the original USB Condom. We listened and spent some time designing and manufacturing our own enclosure.

SyncStop works with any mobile device:



Dr Stephen Hill

26

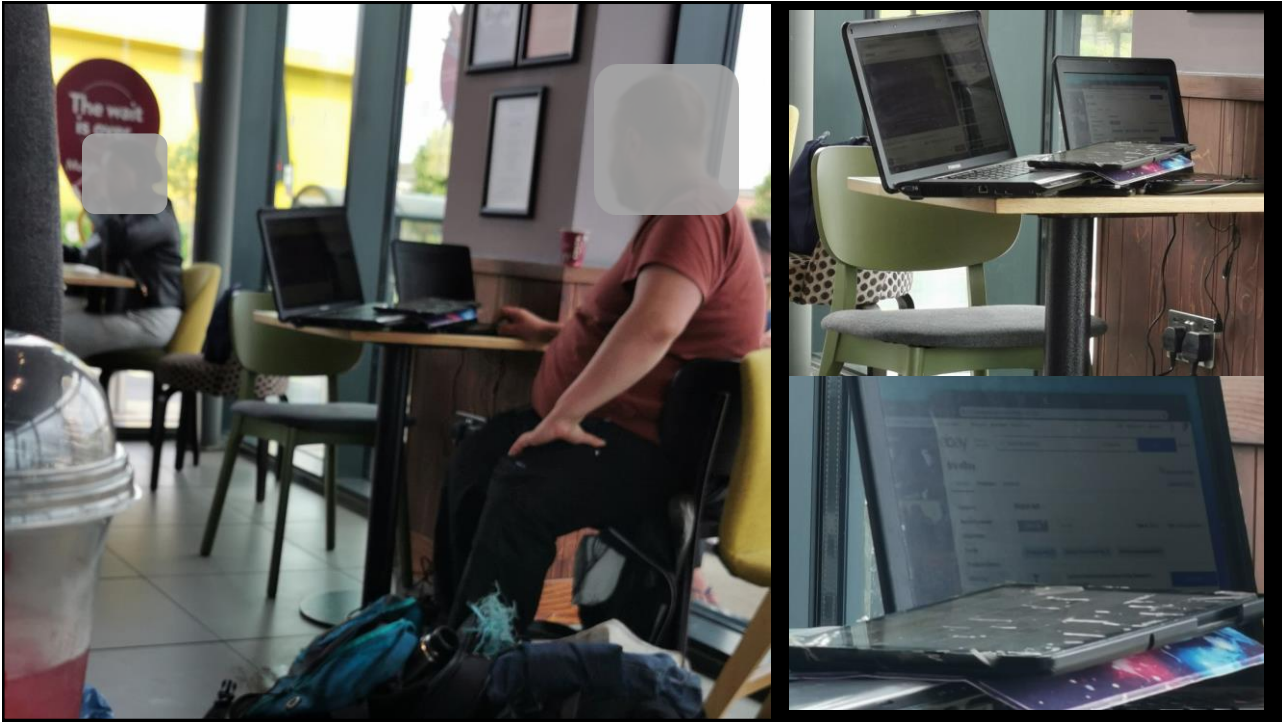


WiFi Hotspots

Croner-i
Inform • Advise • Protect

AIB2021
virtual

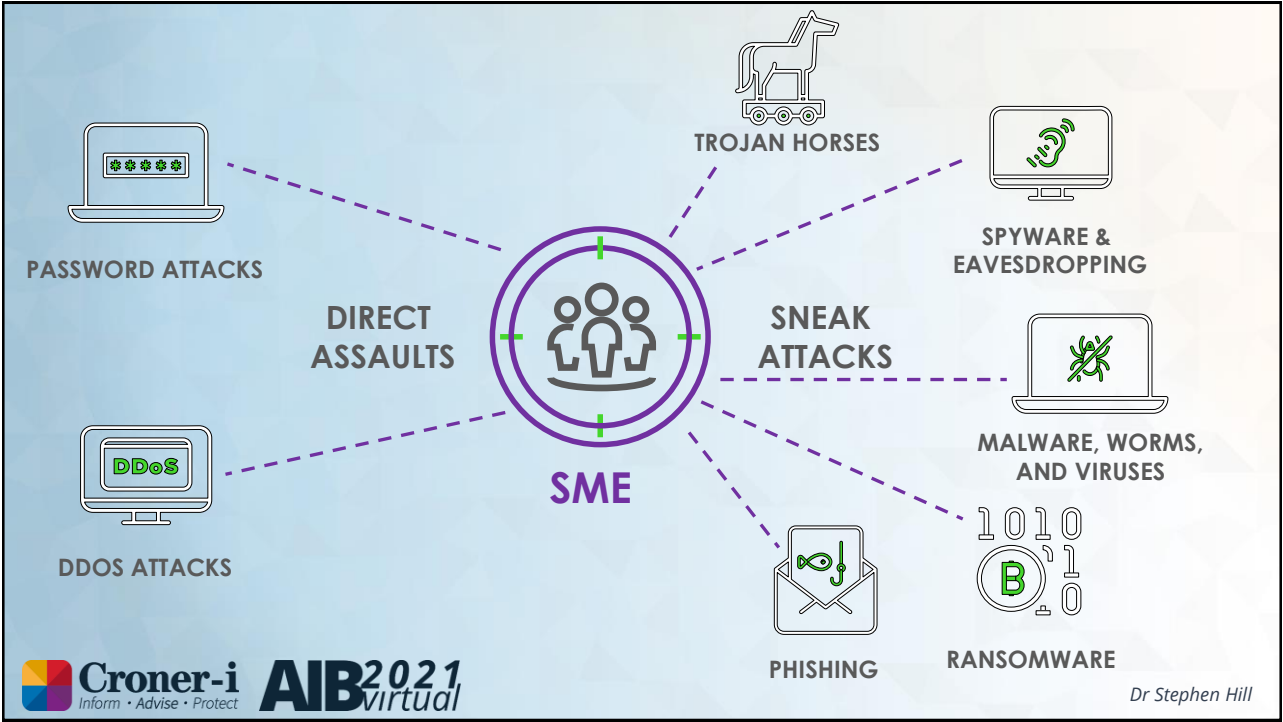
27



28



29



30

Common Misconceptions

Misconceptions are reflected in what SMEs are saying:


‘ WE HAVE ANTI-VIRUS SOFTWARE. ’

‘ OUR DATA IS IN THE CLOUD. (SO IT’S SAFE RIGHT?) ’

‘ WE’RE TOO SMALL TO BE TARGETED. ’


‘ WE DON’T HAVE ANYTHING HACKERS WANT. ’

‘ AN ATTACK/BREACH WON’T HAPPEN TO US. ’



WannaCry

Malware

 **Croner-i**
Inform • Advise • Protect **AIB2021**
virtual

Malware

- “Malware” is the shortened form for ‘malicious software’, which is intrusive software, used to perform actions such as interrupting computer operations and obtaining sensitive information
- Acquiring access to private computer systems and brandishing unsolicited advertising are also characteristic of Malware...

Windows 10 Flaw Lets Malware Disguise Itself as Legit Software

BY MICHAEL KAN 14 JAN 2020, 8:10 P.M.

The National Security Agency is urging users, especially enterprises, to install the patch from Microsoft. In the wrong hands, the vulnerability can be used to spoof the digital certificates software companies use to verify that their applications are authentic.



The US National Security Agency has warned Microsoft about a vulnerability in **Windows 10** that can be abused to make **malware** look like a legitimate program.

On Tuesday, Microsoft released a **patch** to fix the flaw, which also affects Windows Server 2016 and Windows Server 2019. The “spoofing vulnerability” involves the operating system’s CryptoAPI, also known as Crypt32.dll, which can be used to encrypt and decrypt data.

<https://uk.pcmag.com/windows-10/124501/windows-10-flaw-lets-malware-disguise-itself-as-legit-software>

Ransomware

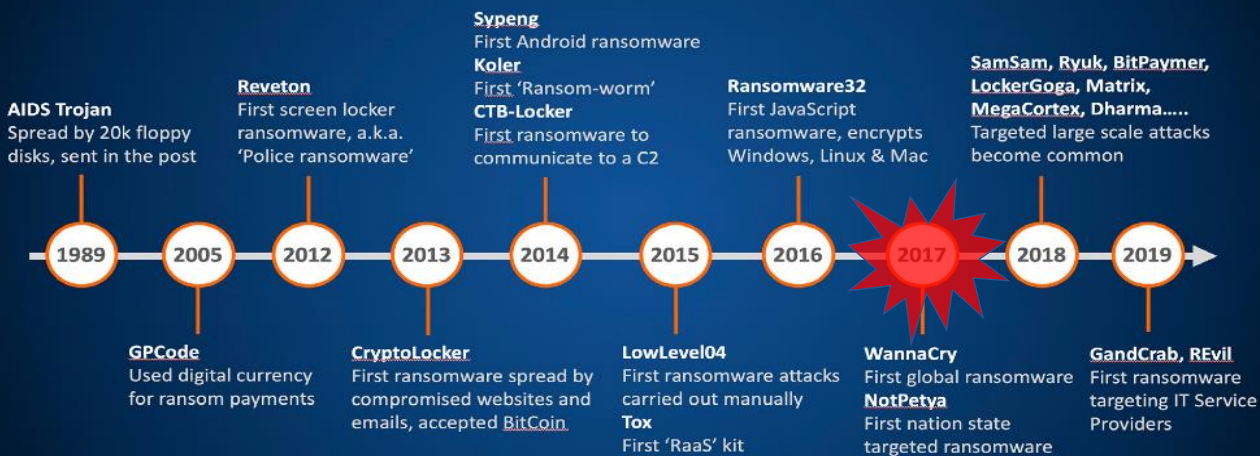
What is Ransomware?

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail.

Today, ransomware authors order that payment be sent via cryptocurrency or credit card...

Ransomware Evolved



WannaCry



Ransomare 2020

61% of organizations were infected with ransomware in 2020

6 days companies impacted lost an average of six working days to downtime

37% said the downtime lasted one week or more

52% of ransomware victims paid threat actors ransom demands

65% only 65% recovered their data

35% never saw their data again despite paying the ransom

In 2020 Travelex the money exchange firm was hit with a file-encrypting malware attack which shut down its internal networks, website and apps for several weeks

Reportedly Travelex paid a ransom of \$2.3 million in BTC to the dark actors to regain access to their data and restore services...

Travelex Paid \$2.3 Million to Ransomware Gang: Report

Attack Crippled Currency Exchange's Services for Weeks

Akshaya Asokan (@asokan_akshaya) · April 10, 2020



- Norsk Hydro the Norwegian energy company experienced a ransomware attack in 2019, it refused to pay
- Instead, the company decided to consult supply chain cybersecurity experts to inspect 30,000 employee credentials and get to the root of the attack
- By taking responsibility and steps to better protect their systems in the future, the company saved reputational damage and put themselves in a better position if another attack occurs...



Hackers hit Norsk Hydro with ransomware. The company responded with transparency

WHAT IS THE IMPACT OF DOWNTIME?

WHEN IT COMES TO RANSOMWARE ATTACKS, MSPs* REPORT THE COST OF DOWNTIME IS

53X

GREATER THAN THE RANSOM REQUESTED

DATA'S RESALE VALUE DOESN'T MATTER WHEN IT COMES TO RANSOMWARE

Ransomware attackers don't need to be able to monetise stolen data, they just need the victimised business to require their data enough to pay to get it back.

'20% of MSPs reported that SMEs were forced to pay a ransom in order to return to normal business.'



* Managed Service Providers
Source: Datto 2020 State of the Channel Ransomware Report
Dr Stephen Hill

INDUSTRIES AFFECTED

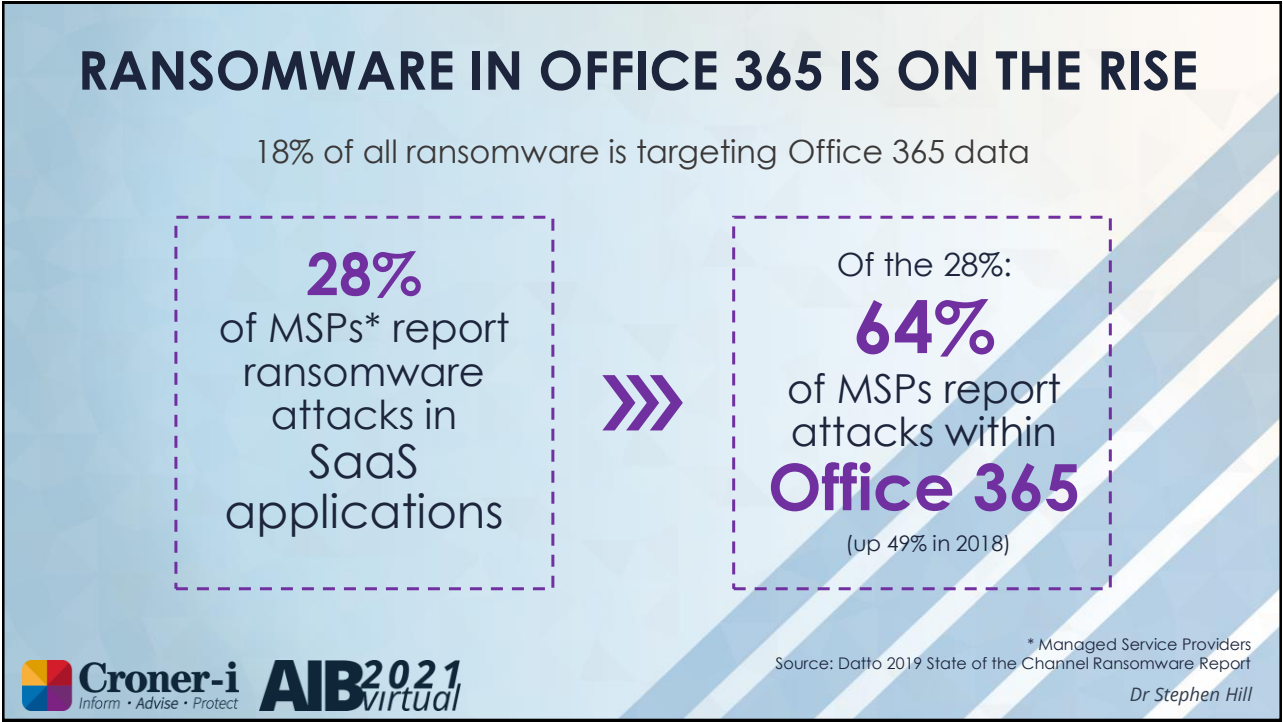
Industries most susceptible to ransomware due to COVID-19:

59%
OF MSP's* REPORT
HEALTHCARE
MOST SUSCEPTIBLE
TO RANSOMWARE

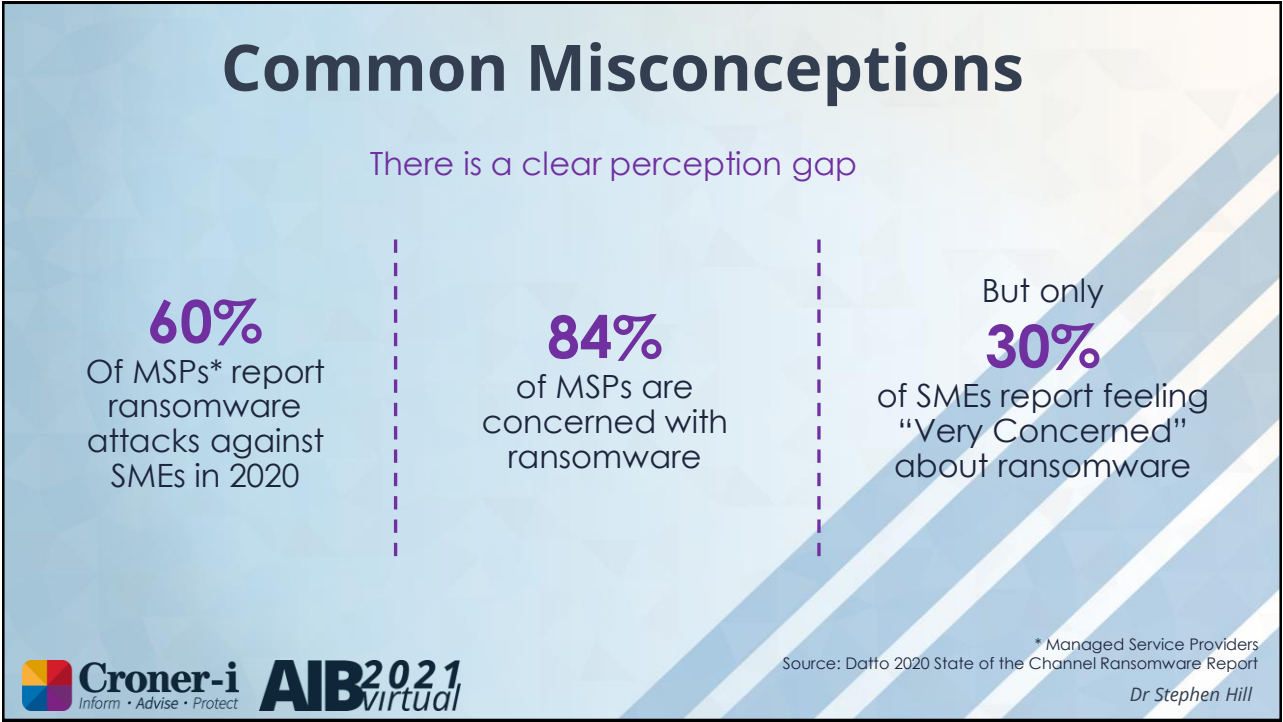
- 50% Finance/Insurance
- 45% Government
- 41% Professional Services
- 36% Education
- 35% High Technology
- 35% Legal
- 29% Non-Profit
- 29% Energy/Utilities
- 27% Retail
- 25% Construction/Manufacturing
- 23% Real Estate
- 22% Travel Transportation
- 22% Telecom
- 22% Media/Entertainment
- 18% Consumer Products
- 17% Architecture/Design
- 7% Other



* Managed Service Providers
Source: Datto 2020 State of the Channel Ransomware Report
Dr Stephen Hill



43



44

Ransomware Advice

<https://www.nomoreransom.org>

NO MORE RANSOM!

Crypto Sheriff Ransomware GBA Prevention Advice Decryption Tools Report a Crime Partners About the Project

DECRYPTION TOOLS

IMPORTANT! Before downloading and starting the solution, read the how-to guide. Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.

Quick Search:

All Ransom (alphabetical order):

- > 777 Ransom
- > AES_NI Ransom
- > Agent.ih Ransom
- > Alcatraz Ransom

PREVENTION ADVICE

WannaCry additional prevention advice

- 1 Disable smb v1, this prevents WannaCry from spreading within your network.
- 2 Install the Microsoft patches, this also prevents WannaCry from spreading within your network. For more information click [here](#)

How to prevent a ransomware attack?

- 1 **Back-up Back-up Back-up!** Have a recovery system in place (so a ransomware infection can't destroy your personal data forever). It's best to create two back-up copies: one to be stored in the cloud (remember to use a service that makes an automatic backup of your files) and one to store physically (portable hard drive, thumb drive, extra laptop, etc.). Disconnect these from your computer when you are done. Your back up copies will also come in handy should you accidentally delete a critical file or experience a hard drive failure.
- 2 Use robust antivirus software to protect your system from ransomware. Do not switch off the 'heuristic' functions as these help the solution to catch samples of ransomware that have not yet been formally detected.
- 3 **Keep all the software on your computer up to date.** When your operating system (OS) or applications release a new version, install it. And if the software offers the option of automatic updating, take it.
- 4 **Think no one.** Literally. Any account can be compromised and malicious links can be sent from the accounts of friends on social media, colleagues or an **online gaming** partner. Never open attachments in emails from someone you don't know. Cybercriminals often distribute fake email messages that look very much like email notifications from an online store, a bank, the police, a court or a tax collection agency, luring recipients into clicking on a malicious link and releasing the malware into their system.
- 5 **Enable the 'Show file extensions' option in the Windows settings on your computer.** This will make it much easier to spot potentially malicious files. Stay away from file extensions like '.exe', '.vbs' and '.scr'. Scammers can use several extensions to disguise a malicious file as a video, photo, or document (like hot-checks an exe or doc scr).
- 6 If you discover a rogue or unknown process on your machine, disconnect it immediately from the internet or other network connections (such as home Wi-Fi) - this will prevent the infection from spreading.

* The general advice is not to pay the ransom. By sending your money to cybercriminals you'll only confirm that ransomware works, and there's no guarantee you'll get the decryption key you need to return.

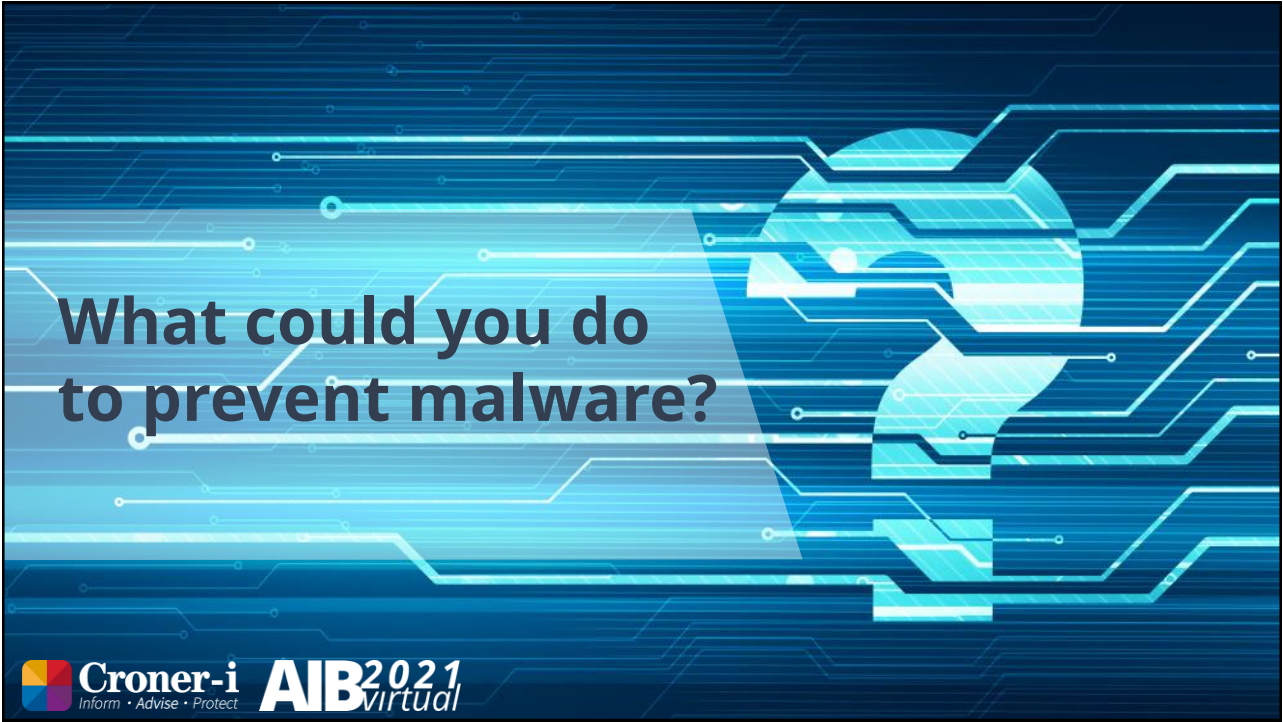
45

Should I pay the ransom?

The National Crime Agency generally advise not to pay the ransom, as there is no guarantee that you will get access to your device (or data)...



46



47

6 TIPS TO PREVENT POTENTIAL RANSOMWARE ATTACKS

 <p>1 Keep your computer patched and up to date.</p>	 <p>4 Don't click the links.</p>
 <p>2 Use an anti-virus scanner.</p>	 <p>5 Practice safe browsing habits.</p>
 <p>3 Use a firewall.</p>	 <p>6 Back up your files.</p>



Dr. Stephen Hill

48



Phishing

Croner-i **AIB2021**
Inform • Advise • Protect virtual

The graphic features a central globe with three red fishing hooks superimposed over it. The background is a dark blue with glowing binary code (0s and 1s) and light trails, suggesting a digital or cyber environment.

49



Email scrutiny -
what would make
you suspicious?

Croner-i **AIB2021**
Inform • Advise • Protect virtual

The graphic has a blue background with a complex circuit board pattern. A large, stylized question mark is positioned on the right side, partially overlapping the circuitry. The text is on the left side, with 'Email scrutiny' in yellow and the rest in white.

50

- Make it difficult to get caught
- The key signs of a phishing attack
- What to do if you took the bait!

Dr. Stephen Hill

51

Simple BUT effective

Dr. Stephen Hill

52

Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

TAKE THE QUIZ



<https://phishingquiz.withgoogle.com>

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr Stephen Hill

53

Don't forget SMS Attacks



Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr. Stephen Hill

54



WiFi Risks

Croner-i
Inform • Advise • Protect

AIB2021
virtual

55





onlinesecurity

Don't use public Wi-Fi to transfer sensitive information such as payment details

Free WiFi
Password:



For more information about how to stay safe online, visit Cyberaware.gov.uk

Croner-i
Inform • Advise • Protect

AIB2021
virtual

Dr. Stephen Hill

56

FBI warns against using free WiFi networks while traveling

FBI: Use your phone's mobile data connection instead.

By [Catalin Cimpanu](#) for [Zero Day](#) | December 18, 2019 -- 18:44 GMT (18:44 GMT) | Topic: [Security](#)

UAE

Crime Education Environment Government Year of the 50th Health Transport Science

Dubai Police warn of public WiFi scams

Cybercriminals create free WiFi networks in malls to steal data of users

Published: August 03, 2017 19:15
Ali Al Shouk, Staff Reporter

Evening Standard

CULTURE INSIDER THE ESCAPIST THE REVELLER THE OPTIMIST COMMENT

NEWS > CRIME

Cyber-criminals 'hack into free wi-fi hotspots to get bank details'

57

Man-in-the-Middle Attack

- One of the dangers of using a public Wi-Fi network is that data over this type of open connection is often unencrypted and unsecured, leaving you vulnerable to a man-in-the-middle (MITM) attack
- MITM is when a cybercriminal exploits a security flaw in the network to intercept data
- This gives a hacker access to sniff out any information that passes between you and the websites you visit — details of browsing activities, account logins, and purchase transactions
- Your sensitive information, such as passwords and financial data, are then vulnerable to identity theft...

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr Stephen Hill

58

CYBERSECURITY LINGO

MAN-IN-THE-MIDDLE-ATTACK

Definition: An approach in which a hacker poses as a user's legitimate destination in order to intercept communications

Short term: **MITM**

Source: slate.com

The diagram shows a VICTIM laptop on the left and a WEB SERVER on the right. A green line labeled 'ORIGINAL CONNECTION' with a green checkmark icon connects them. A red line labeled 'MITM CONNECTION' with a red 'X' icon connects the VICTIM laptop to an ATTACKER laptop positioned below the original connection. The ATTACKER laptop is also connected to the WEB SERVER, effectively intercepting the communication between the victim and the server.

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr Stephen Hill

59

Rogue Hotspots

- Another risk of using free public Wi-Fi is that you may be connecting via a rogue hotspot
- This is an open hotspot, usually with a name similar to that of a legitimate hotspot, which cybercriminals set up to lure people into connecting to their network
- Once a victim connects to the rogue Wi-Fi hotspot,
 - the host hacker can then intercept data and even
 - use tools to inject malware into the connected devices...

The illustration shows a circular Wi-Fi network selection interface. At the top, it says 'USE A NETWORK...'. Below that, there are two entries for 'Coffee Shop' and one for 'Other...'. Each entry has a lock icon to its right, indicating security status.

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr Stephen Hill

60

What do you need to do to stay safe when using public WiFi?

Croner-i Inform • Advise • Protect **AIB2021** virtual

61

360 TOTAL SECURITY

Public Wifi

Security tips to stay safe from hidden dangers

<https://blog.360totalsecurity.com/en/public-wifi-security-tips-stay-safe-hidden-dangers>

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr. Stephen Hill

62

Wifi security tips for home networks

- Update devices and software & apply security patches
- Disable file sharing
 - try to avoid doing this in a public place
 - create a directory for file sharing and restrict access to other directories
 - always password-protect anything you share
- Install HTTPS Everywhere
 - open source browser extension that encrypts communications with most websites
- Use a VPN...

Wifi security tips for home networks

- Confirm your ISP is up-to-date
- Avoid public wifi hotspots
- Manually check URLs are secure
 - HTTP URLs use SSL encryption to protect visitors to the site
- Use secure passwords
- Keep antivirus software up to date
- Use multi-layered security
 - Keep your operating system's firewall updated and use two-factor authentication to access your internet accounts...



Increase in Dark Markets

Croner-i **AIB2021**
Inform • Advise • Protect virtual

65

What is the Dark Net?

- The **dark net** is an encrypted network built over the internet which requires specific software and tools to access the network
- The darknet provides privacy to its users
- An example of a darknet is **Tor** or sometimes referred to as the 'Onion router'
- Tor utilises the hidden service protocol to enter everyday internet websites, but also access many hidden sites that cannot be accessed via conventional browsers...



Croner-i **AIB2021**
Inform • Advise • Protect virtual

Dr Stephen Hill

66

What is the Dark Net?

- The **dark web** is a subset of the deep web
- Can be compared to a World Wide Web of darknets like Tor
- Essentially, sites and services running on the darknet constitute the dark web
- The dark web is often referred to as the seedy underbelly of the internet, with shady dealings and criminal activity running unchecked
- There are however others who would use the dark web including law enforcement, journalists, whistle blowers etc...

"The dark web has become a haven for journalists and whistleblowers like Edward Snowden, or even activists protesting against authoritarian regimes."

Darknet Markets

- A *darknet market* or *crypto-market* is a commercial website on the dark Web that operates via darknets, such as Tor or I2P
- They function primarily as **black markets**, selling or brokering transactions involving:
 - Drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the sale of legal products
- It is the perfect platform to find and buy stolen financial data...

<https://en.wikipedia.org>

The screenshot shows a web browser window with the URL `trdealmgn4uvm42g.onion/listing/3600`. The page header includes navigation links like Home, My RealDeal, Support, and Logout, along with a user balance of BTC 0.0000. The main content area features a listing for 'LinkedIn 167M' by user 'peace_of_mind' (100.0% rating, Level 1/14). The price is listed as 0.5.0000 / BTC 5.0000, and it is currently 'In stock'. A 'Postage Option' dropdown menu is visible. A 'Buy It Now' button is prominent, along with 'Favorite' and 'Question' buttons. The listing details specify 'Escrow: Yes, escrow by RealDeal is available.', 'Class: Digital', and 'Ships From: Worldwide'. The footer contains the 'Croner-i' logo with the tagline 'Inform · Advise · Protect', the 'AIB2021 virtual' logo, and the name 'Dr Stephen Hill'.

69

The screenshot displays a grid of various identification documents for sale, including: Australia Physical, Latvia HQ Passport, Sweden ID Scan (KOK...), Israeli HQ Passport, Hawaii ID Scan, Ceska Republika ID, French HQ Passport, and British License and... Each item includes a 'Buy' button and a price in Bitcoin. To the right, a product description for 'Female selfie holding UK passport + bill' is shown. The vendor is 'CardPass (2950) (4.85★) (@ 146/4/9)'. The price is '£0.00916 (€52)'. Shipping is 'Worldwide' from 'Worldwide'. The description includes a photo of a woman holding a UK passport and a utility bill. The footer features the 'Croner-i' logo, 'AIB2021 virtual' logo, and 'Dr Stephen Hill'.

70

The screenshot shows a web browser window with the URL 'onion/offer/17831'. The page features a navigation bar with links for Home, User-CP, Support, Refrally, Quality control, and Log Out. The main content area is titled 'Info' and includes a vendor name, a button for 'Any questions about the offer?', and checkboxes for 'Digital goods' and 'Escrow'. On the right, there is a Bitcoin logo, an 'Add to favorites' button, and a purchase section with an 'Amount' field set to '1' and a 'Buy' button. Below the purchase section, it says 'Scroll down for prio'. The offer title is '[Pack id] Scan French CNI + Passeport réel de la même personne'. There are two tabs: 'Description' (selected) and 'Refund policy & Vendor information'. The description text reads: 'Pack de scans : Carte d'identité Française + Passeport Français réels de la même personne. Valides et jamais utilisés. Idéal pour ouvrir des comptes Czam , Pcs et bien d'autres...'. Below this, it states: 'Scans : real French National ID + real French Passport of the same person , never sold and never used.' At the bottom left, there are logos for 'Croner-i' (Inform · Advise · Protect) and 'AIB2021 virtual'. At the bottom right, the name 'Dr Stephen Hill' is displayed.

71

The graphic features the text 'Social Media Risks' in white on a black background. To the right, there is a close-up, 3D-rendered image of a computer mouse clicking a blue 'Add as Friend' button. At the bottom left, there are logos for 'Croner-i' (Inform · Advise · Protect) and 'AIB2021 virtual'.

72

Can you name a risk linked to the use of social media?

Croner-i
Inform • Advise • Protect

AIB2021
virtual

73

Social Media Security Threats

- Leaving Footprints
- Malware attacks and hacks
- Third-party apps
- Human error
- Phishing attacks and scams
- Privacy settings
- Imposter account
- Unsecured mobile phones

Croner-i
Inform • Advise • Protect

AIB2021
virtual

Dr. Stephen Hill

74

The information you share can often answer security questions. Which information do people share the most?

Information Type	Percentage
birthdays	63%
schools	61%
family members	51%
hometowns	48%
favorite TV shows	44%
favorite musicians	38%
favorite books	33%
vacation plans	26%
pets' names	23%

Over-sharing Information

Scammers and hackers often use these details to create targeted phishing emails that could expose your computer to viruses or get you to reveal login details for your email account, social media profiles, or bank accounts...

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr Stephen Hill

75

Fake Accounts/Connection Requests

- One of the more elaborate schemes that's becoming increasingly popular is the creation of fake accounts that send friend or connection requests to users within the network
- Once a fake account is connected to a user, it's relatively easy to trick the user into clicking a malicious link...

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr Stephen Hill

76

Fake Accounts/Connection Requests



Mia Ash
 Photographer at Mia's Photography
 London, Greater London, United Kingdom | Photography

500+ connections

Current: Mia's Photography
 Previous: Loft Studios, Clapham Studios
 Education: Goldsmiths, University of London



Mia Ash
 Photographer at Mia's Photography
 London, Greater London, United Kingdom | Photography

Current: Mia's Photography
 Previous: Loft Studios, Clapham Studios
 Education: Goldsmiths, University of London

157 views
 @miamash2014 alert
 #photography #photographer #photography #miamash

Once a fake account is connected to a user, it's relatively easy to trick the user into clicking a malicious link.

This is just what happened in 'The Curious Case of Mia Ash', a fake LinkedIn persona that was designed to establish relationships with employees at targeted organisations...

Social Media & Metadata Footprints



Where is she??

Croner-i
Inform • Advise • Protect

AIB2021
virtual

Dr. Stephen Hill

79

Follow the evidence

197 views 7 faves 0 comments Taken on May 2, 2021

© All rights reserved

OLYMPUS E-620
Olympus Zuiko Digital 40-150mm F3.5-4.5

f/8.0 1/640
 ISO 200 Flash (auto, did not fire)
 Show EXIF

CALIF: Las Vegas
Los Angeles ARIZ. N.M.

Cross Roads, California, United States

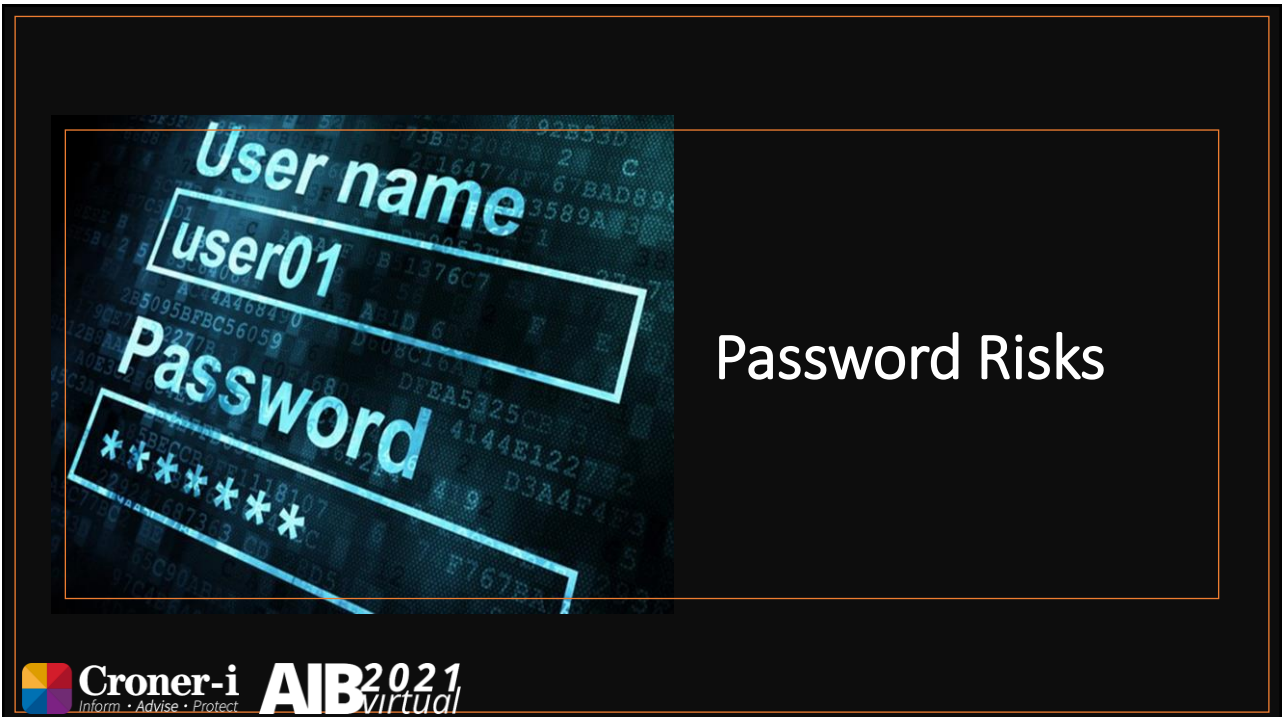
Add a comment

80

Key Points to Remember When Using Social Media Sites

- DON'T over-share personal information
- DON'T click on suspicious links or posts
- DON'T accept connection requests from people you don't know
- DO use strong, unique passwords for each platform
- DO use two-factor authentication whenever possible
- DO regularly check your privacy settings on each social platform
- DO check which third-party apps have access to your social media profiles
- DO actively monitor your social media accounts
- DO educate yourself and your employees on social media attacks and threats

81



Password Risks


82


SECURITY

Gates predicts death of the password



Traditional password-based security is headed for extinction, says Microsoft's chairman, because it cannot "meet the challenge" of keeping critical information secure.

BY MUNIR KOTADIA | FEBRUARY 25, 2004 1:27 PM PST





Dr. Stephen Hill





83

How a Password is Hacked


Key Logging


An installed keylogger intercepts passwords as they are typed.




Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.








Brute Force



Automated guessing of billions of passwords until the correct one is found.

Interception

Passwords can be intercepted as they are transmitted over a network



Dr. Stephen Hill

84

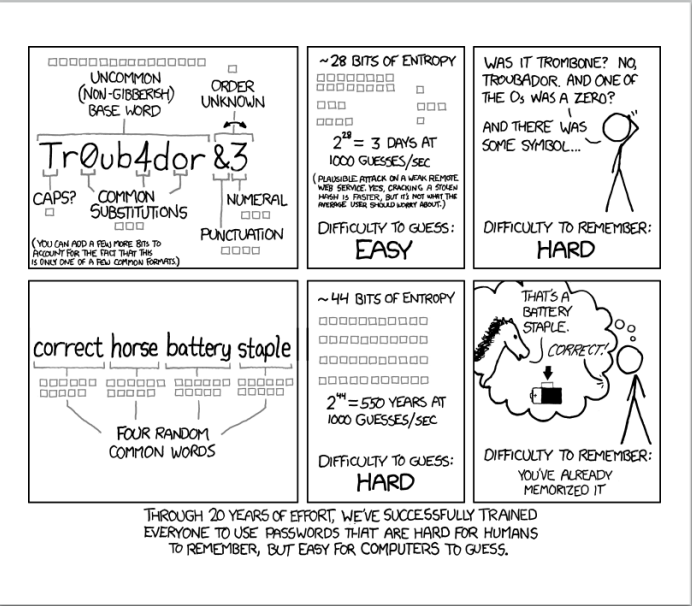
What makes a secure password & do you have a password policy?



Croner-i Inform • Advise • Protect **AIB2021** virtual

85

The Password Dilemma



Method 1: Complex Password

- UNCOMMON (NON-GIBBERISH) BASE WORD
- ORDER UNKNOWN
- Tr0ub4dor&3
- CAPS? COMMON SUBSTITUTIONS NUMERICAL PUNCTUATION
- (YOU CAN ADD A FEW MORE BITS TO PROBABLY GET THE FEEL THAT THIS IS ONLY ONE OF A FEW COMMON EXAMPLES)
- ~28 BITS OF ENTROPY
- $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$
- (PLAUSIBLE ATTACK ON A WEAK PASSWORD: YES. SERVICE YES. COMING IN STRONG AGAIN IS FASTER, BUT IT'S NOT WHAT THE PROBLEM USER SHOULD WORRY ABOUT.)
- DIFFICULTY TO GUESS: **EASY**
- DIFFICULTY TO REMEMBER: **HARD**

Method 2: Common Words

- correct horse battery staple
- FOUR RANDOM COMMON WORDS
- ~44 BITS OF ENTROPY
- $2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$
- THAT'S A BATTERY STAPLE. CORRECT!
- DIFFICULTY TO GUESS: **HARD**
- DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Croner-i Inform • Advise • Protect **AIB2021** virtual

86

Campaign by the National Cyber Security Centre (NCSC)

Three random words or #thinkrandom

Ian M discusses what makes a good password



WRITTEN BY Ian M

PUBLISHED 27 October 2016

WRITTEN FOR Individuals & families, Self employed & sole traders, Small & medium sized organisations, Large organisations, Public sector

PART OF BLOG Inside the NCSC



- Download PDF
- Share
- Print

You're probably aware that there's a lot of guidance out there on what makes a good password – and it can be incredibly confusing. This blog post should help.

For home users we are working with Cyber Aware, advising that you create passwords using three random words. You just put them together, like 'coffeetrainfish' or 'wolltinshirt'.



<https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0>

87

Secure password generator to help keep you safer online

Canyon-Miss-Scientific-Anywhere-5 Length: 33

Min words: 4

Min Length: 20 (including the separator)

Separator: - (Multiple values will be used randomly, try * & ^ % \$!)

Make First Letter Uppercase

Append random number to the end (0 - 9)

Save these options.*

Additional dictionaries

Jargon file

Science terms

Generate password Copy link



<https://correcthorsebattery Staple.net>

Dr. Stephen Hill

88

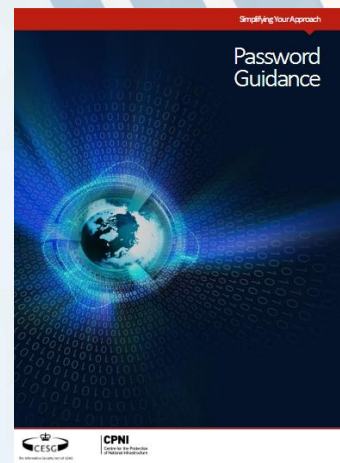
How Can Businesses Protect Passwords?

The NCSC has outlined four ways that businesses can improve system security:

- ALL corporate web apps requiring authentication have HTTPS in place
- Ensure that any access management systems you manage are protected
- Protect access to user databases
- #ThinkRandom
- Prioritise administrators, cloud accounts and remote users...

Password Advice

- Regular password changing harms rather than improves security – so AVOID placing this burden on users!
- BUT – users must change their passwords on indication of suspicion or compromise



Email Exposed?

<https://breachalarm.com>

Dr. Stephen Hill

91

Email Exposed?

<https://haveibeenpwned.com>

Dr. Stephen Hill

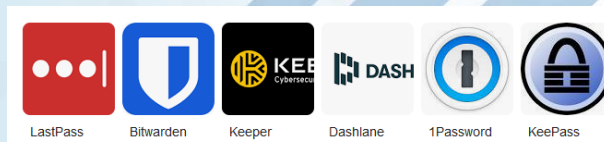
92

Password Management



Password Managers

- According to Keeper Security, 81% of data breaches are due to weak password security with the average cost of a data breach to a company coming in at \$7 million
- Password managers let users create hard-to-break passwords and automatically log in to websites without having to remember those passwords
- Many also analyse the strength of passwords, monitor accounts for data breaches, and provide secure private browsing networks...



Password Managers



The 7 Best Password Managers of 2021

- Best Overall: [LastPass](#)
- Best for Extra Security Features: [Dashlane](#)
- Best Multi-Device Platform: [LogMeOnce](#)
- Best Free Option: [Bitwarden](#)
- Best for New Users: [RememBear](#)
- Best for Families: [1Password](#)
- Best Enterprise-Level Manager: [Keeper](#)

95

LastPass... |

[SIGN UP NOW](#)

We chose LastPass as the best overall because it offers a rich set of free features allowing most users to get everything they need without paying anything. It can be accessed on most browsers and virtually all smart devices and also offers more robust sharing features through its paid versions.

✓ Pros

- Easy to use
- Feature-rich free version
- Multi-factor authentication (MFA)

✗ Cons

- Outdated desktop apps
- Can't auto-fill some personal data types
- Website hacked in 2015

LastPass was created in 2008 by four developers tired of having to encrypt and decrypt their password document every time they updated it. By the time it was bought by SaaS company LogMeIn in 2015, it had grown to seven million users supported by just 30 employees.

96



SIGN UP NOW

We chose Dashlane as the best for extra security features because it offers dark web scanning for data leaks, a secure virtual private network (VPN), and a password changer option.

✓ Pros

- Easy syncing between devices
- Built-in VPN
- Dark web monitoring

✗ Cons

- 50 password limit on free plan
- Free plan limited to use on one device
- Limited cloud storage

French-based company Dashlane launched its password manager in 2009 which has quickly risen to become a major player in the marketplace. It offers both a robust free plan and paid plans with additional security support for its customers.

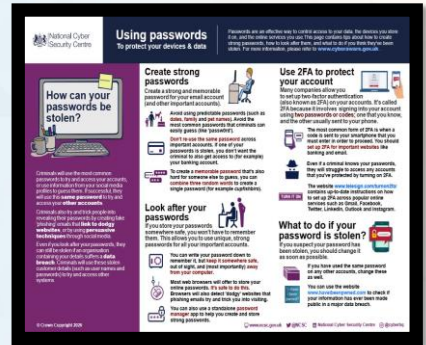


Dr Stephen Hill

NCSC Password Guidance

This Guidance is free and available at the NCSC

- Create Strong Passwords
- Keep Passwords Safe
- Use 2FA
- What to do Password Compromised...



Dr. Stephen Hill

Cyber Risk Management

10101 NAME ADDRESS
 101001010010101101001001
 IN 101 LOGIN **PASSWORD**
 101001010010101101001001
 101010 NAME ADDRESS
 101001010010101101001001
 1010101011010101101011010
 101001010010101101001001

Croner-i **AIB2021**
 Inform • Advise • Protect virtual

99

What is Cyber Security?


Cyber Security is the protection of devices, services and networks - and the information on them – from theft or damage via electronic means.

Croner-i **AIB2021**
 Inform • Advise • Protect virtual



Dr Stephen Hill

100

Computer Security - checklist




- Harden your devices
 - No matter which OS used always keep it up to date
 - **Passwords** – multi factor authentication
 - Limit the number of applications running on a device
- Antivirus & Malware
 - Use real-time applications
 - Run both – anti-malware differs from anti-virus
 - Ensure the use of a firewall on mobile devices
- Physical Security
 - Consider disconnecting camera(s) and microphone
 - Encrypt and **wipe devices** before recycling
 - Turn off **WiFi** & Bluetooth...

Dr. Stephen Hill

101




10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.



10 Steps

- Network Security**
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.
- User education and awareness**
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.
- Malware prevention**
Produce relevant policies and establish anti-malware defences across your organisation.
- Removable media controls**
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before reporting onto the corporate system.
- Secure configuration**
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



- Managing user privileges**
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
- Incident management**
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report critical incidents to law enforcement.
- Monitoring**
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.
- Home and mobile working**
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk [@ncsc](https://twitter.com/ncsc)

Dr. Stephen Hill

102

NCSC Guidance

National Cyber Security Centre

What you can do to combat cyber attacks

Reducing The Impact
Most cyber attacks are composed of four stages: **Survey, Delivery, Breach and Affect**. The following **security controls**, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey

User Education
Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Delivery

Network Perimeter Defences
Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection
Can block malicious emails and prevent malware being downloaded from websites.

Password Policy
Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration
Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

Breach

Patch Management
Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring
Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection
Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration
Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access
Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training
User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls
Devices within the internet gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Affect

Controls For The Affect Stage
Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help. **10 Steps To Cyber Security** outlines many of the features of a complete cyber risk management regime.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find tinkering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

£600K-£1.15m

Average cost of security breach

81%

of large companies reporting breach

For more information go to www.ncsc.gov.uk @ncsc

Croner-i
Inform • Advise • Protect

AIB²⁰²¹ virtual

Dr Stephen Hill

103

Breach

Patch Management
Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring
Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection
Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration
Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access
Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training
User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls
Devices within the internet gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Croner-i
Inform • Advise • Protect

AIB²⁰²¹ virtual

Dr. Stephen Hill

104



105

Setting Up New Accounts

- Many organisations will be setting up new accounts allowing staff to work from home
- When setting up a new account consider the following:
 - Strong passwords
 - 2FA (Two-Factor Authentication)*

* Double checking the person trying to login in is genuine...

106

How do I set up 2FA?

- Some online services will already have 2FA switched on by default
- The option to switch on 2FA is usually found in the security settings of the account (where it may also be called 'two-step verification')
- The website www.telesign.com/turnon2fa/tutorials contains instructions on how to set up 2FA across many popular online services
- You can also visit the site for more information on 2FA such as Twitter for example
 - <https://help.twitter.com/en/managing-your-account/two-factor-authentication...>

Data Exposure - Risk & Remedy


- Remote workers are more likely to have their devices stolen (or lose them) when they are away from the office
- Make sure devices encrypt your data which will protect your company data on the device if it is lost or stolen
- Today most modern devices have encryption built in, but it may need to be turned on and configured
- Most devices include tools that can be used to remotely lock access to the device, erase the data stored on it, or retrieve a backup of this data. ...



Encryption



Croner-i **AIB2021**
Inform · Advise · Protect virtual

109

Encryption & Decryption




Encryption



Decryption


Plaintext **Ciphertext** **Plaintext**

Croner-i **AIB2021**
Inform · Advise · Protect virtual

Dr Stephen Hill

110

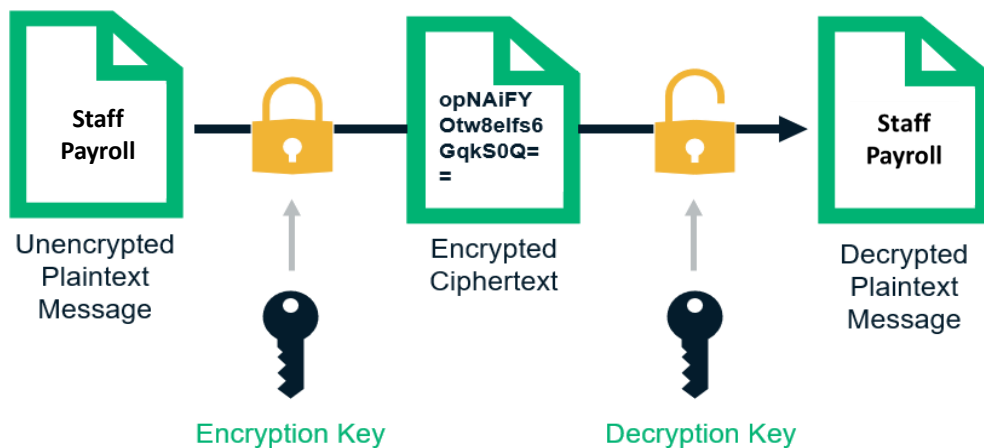
Encryption

- Encryption is the conversion of meaningful text (plaintext) into meaningless text (cipher text) in a manner that can be reversed by anyone with the encryption key
- Encryption protects information stored on mobile and static devices and in transmission
- It is a way of safeguarding against unauthorised or unlawful processing of data
- Organisations should consider encryption alongside other technical and organisational measures, taking into account the benefits and risks that it can offer...

<https://ico.org.uk>

111

How Encryption Works



112

The screenshot shows the Microsoft Windows Support website. The navigation bar includes links for Office, Windows, Surface, Xbox, Deals, Support, and More. The main content area is titled "Turn on device encryption" and includes a sub-header "Device encryption helps protect your data by encrypting it. Only someone with the right encryption key (such as a password) can decrypt it. Device encryption is not available in Windows 10 Home." Below this, there is a numbered list of four steps: 1. Sign in to Windows with an administrator account. 2. Select the Start button, then type manage BitLocker. 3. Select Manage BitLocker from the list of results. 4. Select Turn on BitLocker, then follow the instructions. A link "If you need to decrypt your PC, find your recovery key." is provided at the end of the list. The footer contains the Croner-i logo, AIB2021 virtual logo, and the name Dr. Stephen Hill.

113

The screenshot shows the Microsoft Windows Support website. The navigation bar includes links for Office, Windows, Surface, Xbox, Deals, Support, and More, along with search, shopping cart, and sign in icons. The main content area is titled "How to encrypt a file" and includes a sub-header "File encryption helps protect your data by encrypting it. Only someone with the right encryption key (such as a password) can decrypt it. File encryption is not available in Windows 10 Home." Below this, there is a numbered list of three steps: 1. Right-click (or press and hold) a file or folder and select Properties. 2. Select the Advanced button and select the Encrypt contents to secure data check box. 3. Select OK to close the Advanced Attributes window, select Apply, and then select OK. On the right side, there are links for "Email", "Print", and "Subscribe RSS Feeds". At the bottom left of the content area, it says "Last Updated: 20 Nov 2017". The footer contains the Croner-i logo, AIB2021 virtual logo, and the name Dr. Stephen Hill.

114

Mac FileVault 2

Use FileVault to encrypt the startup disk on your Mac

FileVault full-disk encryption (FileVault 2) uses XTS-AES-128 encryption with a 256-bit key to help prevent unauthorized access to the information on your startup disk.

Turn on FileVault Reset password Turn off FileVault

Croner-i *Inform • Advise • Protect* **AIB2021** *virtual*

Dr. Stephen Hill

115

Internet Privacy

Internet Privacy

Croner-i *Inform • Advise • Protect* **AIB2021** *virtual*

116





119

How Transparent are You?

<https://panoptick.eff.org>

A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION
DONATE

PANOPTICK

Is your browser safe against tracking?

When you visit a website, online trackers and the site itself may be able to identify you - even if you've installed software to protect yourself. It's possible to configure your browser to thwart tracking, but many people don't know how.

Panoptick will analyze how well your browser and add-ons protect you against online tracking techniques. We'll also see if your system is uniquely configured—and thus identifiable—even if you are using privacy-protective software.

TEST ME

Only *anonymous data* will be collected through this site.

Panoptick is a research project of the Electronic Frontier Foundation. [Learn more](#)

A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION

[ABOUT PANOPTICK](#)
[DONATE TO EFF](#)
[CONTACT](#)
[PRIVACY](#)
[CC-LICENSE](#)

120

Dr. Stephen Hill

Think before you Search

- Major search engines tend to use cookies on devices to track what you are searching for on the Internet and what you might be interested in
- The main aim of this form of tracking is to profile web users and use the collected information to send targeted ads
- Privacy is an issue so is Google safe to use?

121



Careful what you search for ... someone could be looking!

Google Search

I'm Feeling Lucky

Google.ae offered in: العربية فارسی हिन्दी اردو

122



Google tracks you. We don't.

DuckDuckGo.com

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr. Stephen Hill

123

Consider a privacy focused search engine such as StartPage or DuckDuckGo



Startpage.com

The world's **most private** search engine



DuckDuckGo

The search engine that doesn't track you. [Help Spread DuckDuckGo!](#)

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr. Stephen Hill

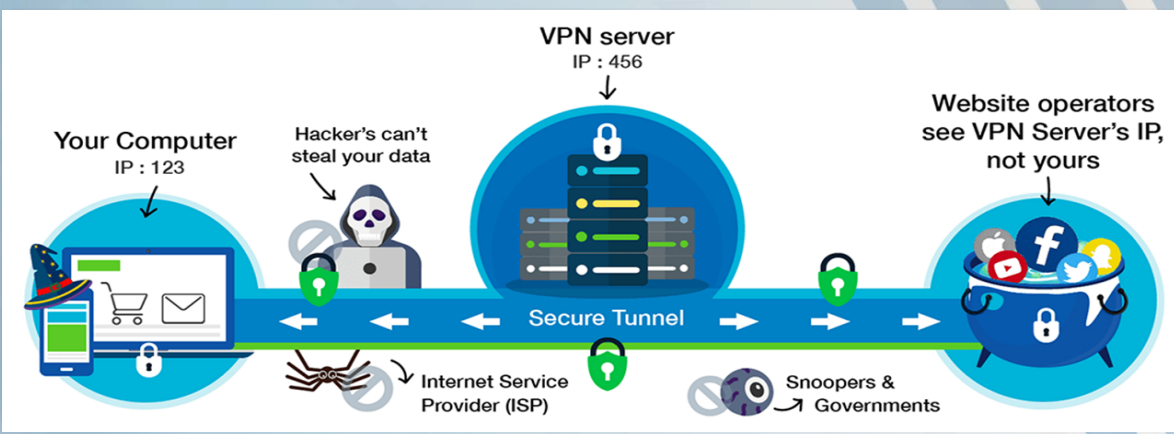
124

Hiding your Identity Online



125

Virtual Private Network (VPN)



Source: 360 Total Security

126

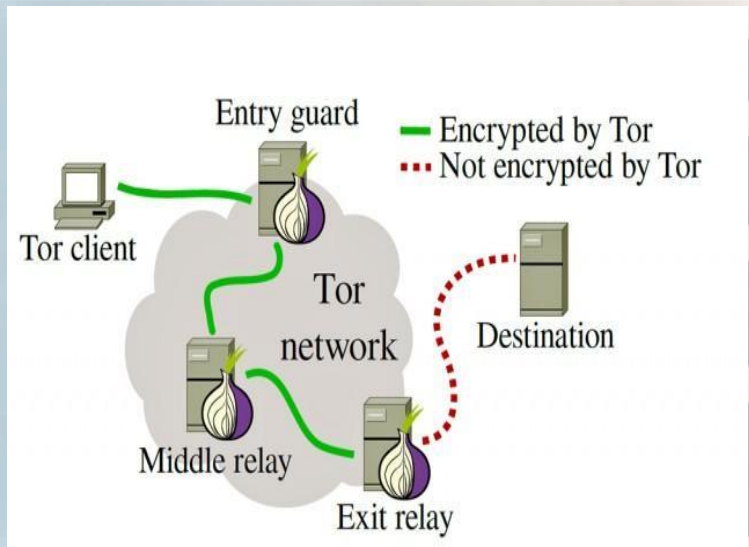
The Onion Router (TOR)

The screenshot shows the Tor Project website. At the top is the Tor logo (an onion) and navigation links: Home, About Tor, Documentation, Press, and Blog. Below this is a green banner with the heading "Anonymity Online" and the text "Protect your privacy. Defend yourself against network surveillance and traffic analysis." A purple button says "Download Tor". To the right, a box lists features: "Tor prevents people from learning your location or browsing habits.", "Tor is for web browsers, instant messaging clients, and more.", and "Tor is free and open source for Windows, Mac, Linux/Unix, and Android". Below the banner are two sections: "What is Tor?" and "Why Anonymity Matters".

What is Tor?
Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Why Anonymity Matters
Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Connecting to Tor



The screenshot shows a web browser window with the address bar displaying `https://www.startpage.com`. A Tor Circuit overlay is visible on the left side of the browser window, showing the connection path: This browser -> France (62.210.177.181) -> Romania (93.115.86.6) -> Germany (185.220.102.7) -> startpage.com. A blue button labeled "New Circuit for this Site" is present. Below the circuit, it states "Your Guard node may not change. Learn more". A "Permissions" section indicates that no special permissions have been granted. The Startpage.com logo and search bar are visible on the right side of the browser window.

129

Look at the URL

https://en-gb.facebook.com

The screenshot shows the Facebook login page with fields for "Email or Phone" and "Password", a "Log In" button, and a "Create an account" section with fields for "First name", "Surname", "Mobile number or email address", and "New password".

The Tor logo, featuring a purple onion, is shown with a large purple arrow pointing downwards towards the alternative URL.

Facebook, Inc.(US) https://www.facebookcorewwi.onion

130

BBC News launches 'dark web' Tor mirror
 © 23 October 2019

The screenshot shows a news article on the left and a browser's Tor circuit diagram on the right. The article title is "BBC News launches 'dark web' Tor mirror" dated 23 October 2019. The article text states: "The BBC has made its international news website available via the Tor network, in a bid to thwart censorship attempts." It explains that the Tor browser is privacy-focused and can help avoid government surveillance. Countries like China, Iran, and Vietnam are mentioned as having tried to block access. The browser's Tor circuit diagram shows the path from the browser through several relays in the US, Finland, and Norway, ending at the destination site.

The BBC has made its international news website available via the Tor network, in a bid to thwart censorship attempts.

The Tor browser is privacy-focused software used to access the **dark web**.

The browser can obscure who is using it and what data is being accessed, which can help people avoid government surveillance and censorship.

Countries including China, Iran and Vietnam are among those who have tried to block access to the BBC News website or programmes.

Tor Circuit

- This browser
- United States 172.92.156.32 **Guard**
- Finland 95.216.99.156
- Norway 37.191.194.50
- Relay
- Relay
- Relay
- bbcnews2vjtpsuy.onion

Croner-i Inform • Advise • Protect **AIB2021** virtual

Dr. Stephen Hill

131

Security Verdict

Run TOR Over VPN

- User first connects to the VPN establishing the secure, encrypted tunnel
- The traffic then passes through the Tor network, and after the encrypted data comes out of the exit node, it's transferred to the VPN server, before it finally makes it way to the Internet
- This makes you more anonymous online as the VPN provider can't see your IP address, and also keeps you safe from malicious nodes because the data is still encrypted when it emerges from the exit node of Tor...

132



133

Get into Good Habits – things to check

- Install the latest software and app updates onto all your devices including mobiles and tablets
 - *They contain vital security updates which help protect your device from viruses and hackers*
- Use a strong, separate password for your email account
 - *Hackers can use your email to access many of your personal accounts, by asking for you password to be reset, and find out personal information, such as your bank details, address or date of birth, leaving you vulnerable to identity theft or fraud*
- Secure your tablet or smartphone with a screen lock
 - *Give your device an extra layer of security by setting it to lock when you aren't using it*
- Always back up your most important data
 - *Safeguard your most important data such as your photos and key documents by backing them up to an external hard drive or a cloud-based storage system...*

134

Get into Good Habits – things to check

- Don't use public Wi-Fi to transfer sensitive information such as card details
 - *Hackers can set-up fake WiFi hotspots, which might enable them to intercept sensitive information you are transferring online*
- Don't 'jailbreak' or 'root' your smartphone
 - *Jailbreaking or rooting turns off software restrictions placed by the manufacturer, allowing you to download and install apps which aren't available through official app stores*
- Beware of fake websites
 - *Cyber criminals can set-up fake websites to try and get you to share sensitive information, such as your bank account details or passwords, or download malware (malicious software) which can infect your device and damage or delete the data you have on it*
- Never click on suspicious links or attachments
 - *Beware of suspicious emails. Even if they seem to come from a company or person you know, contact them by other means to check they are genuine...*



NCSC Links

<https://www.ncsc.gov.uk/information/infographics-ncsc>

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online>

Recommended Guidance

Video conferencing Using services securely

The COVID-19 lockdown means many of us are now using video calls to stay in touch with family, friends and work colleagues. If you're new to video conferencing, this may seem a little daunting. Even if you're familiar with video conferencing, you should take a moment to review how you're using it.



What is video conferencing?

Video conferencing is a live audio and video communication between 2 or more people in different locations. Considered a 'remote' service, it can be used for anything from a meeting to a training session.

Many devices have video conferencing functionality built in (such as Apple's FaceTime and Google's Duo), and many desktop PCs will download the necessary software to allow you to use video conferencing services. You can also use video conferencing apps that you can download (such as Zoom, Skype, Microsoft Teams and WebEx).

For more information about the security features of a specific video conferencing service, please refer to the service provider's official support site. Use a service provider's website carefully as you may be able to download software if you have any problems whilst using the service.

Home working: Managing the cyber risks

Working from home is not new to many of us, but the coronavirus (COVID-19) means organisations are using home working on a greater scale, and for longer periods. This page will only summarise the key risks for home working. It does not provide advice on getting COVID-19 tests done.



Spotting email scams linked to COVID-19

Cyber criminals are preying on fears of COVID-19. Scams are being sent out, often from trusted sources or might encourage you to donate. Be particularly alert to emails from websites which could download viruses into your device, or steal your personal data.

Don't click on any such links. For genuine information about the virus, please see trusted sources such as the Public Health England (PHE) website.

If you're already infected, don't panic:

- Run a virus scanner software on your full PC, following any instructions.
- If you're concerned about your personal information, you should change your passwords on all your other accounts.
- If you're using a work device, contact your IT department for further advice.
- If you have lost money, you need to report it to Action Fraud (0300 123434) or online by visiting www.actionfraud.police.uk

- 1. Downloading video conferencing software**
 - If using standalone video conferencing software, only download it from trusted sources (such as Apple's App Store or Google Play), or from the service provider's official website.
 - Use tech websites and other trusted sources to research which app is right for you. The 'free' version of a video conferencing service will provide good enough security for personal use, provided you've set it up correctly.
 - Check the privacy settings. You should make sure that you understand what (if any) data the service will access during operation. You may have the option to opt out of sharing data.
- 2. Setting up video conferencing services**
 - Make sure that the password for your video conferencing account (or for the device or app you are using for video conferencing) is different to all your other passwords, and difficult for someone to guess. If available, set up two factor authentication (2FA) for the account (and for your device and other apps, if available).
 - Test the service before making or joining your first call. Check that your microphone and camera work, and that your internet connection is fast enough. Learn how to mute your microphone and how to turn off the camera.
 - Many services allow you to record the meeting, share files, or show what is on somebody's screen. Find out how to tell if the call is being recorded.
- 3. Hosting and joining calls**
 - Do not make calls public. Connect directly to the people you want to call using your contact address book, or provide invite links to the individual contacts. If possible set up the call so that a password is required to join.
 - Consider using the lobby feature to ensure you know who has arrived. Make sure people are who they say they are before they join the call, the password function described above can help with this.
 - Think about what your camera shows when you're on a call. Would you expect to share that information with strangers? Consider blurring or changing your background, if you find instructions on how to do this on the support website for your video conferencing service.
- 4. Keep all devices and applications up to date**
 - Make sure that all your devices and applications (and the video conferencing software) are kept up to date. Applying software updates is one of the most important things you can do to protect yourself online.
 - Update all the apps (and your device's operating system) whenever you're prompted. It will add new features and sometimes improve your security.

- 1. Setting up user accounts & access**
 - Set strong passwords for user accounts. Use NCSC guidance on passwords and review your password policy. Implement two-factor authentication (2FA) where available.
- 2. Preparing for home working**
 - Think about whether you need new services, or to just extend existing services so teams can still collaborate. <https://www.ncsc.gov.uk/onlineopenings> can help you choose and roll out a range of popular services. In addition:
 - Consider producing 'How to IT' guides for new services so that your help desk staff aren't overwhelmed with requests for help.
 - Devices are more likely to be stolen (at least when home working). Ensure devices are encrypted whilst at rest. Most modern devices have encryption built in, but may need to be turned on and configured.
 - Use mobile device management (MDM) software to set up devices with a standard configuration in case the device needs to be remotely locked, or have data erased from it.
 - Make sure staff know how to report any problems, or raise support calls. This is especially important for security issues.
 - Staff feeling more exposed to cyber threats when home working should work through the NCSC's [Top Tips for Staff Working Remotely](https://www.ncsc.gov.uk/onlineopenings).
- 3. Controlling access to corporate systems**
 - Virtual Private Networks (VPNs) allow home workers to securely access your organisation's IT resources (such as email). If you've not used one before, refer to the NCSC's [VPN Guidance](https://www.ncsc.gov.uk/onlineopenings), which covers everything from choosing a VPN to the advice you give to staff.
 - If you already use a VPN, make sure it's fully patched. You may need extra licenses, capacity or bandwidth if you're supporting more home workers.
- 4. Helping staff to look after devices**
 - When using their own devices, the organisation's ensure staff understand the risks of using them outside the office. When not used, staff should keep devices somewhere safe.
 - Make sure they know what to do (and who to call) if devices are lost or stolen. Encourage users to report any losses as soon as they can.
 - Ensure staff understand how to keep software and devices up-to-date, and that they update promptly.
- 5. Using removable media safely**
 - USB drives may contain sensitive data. An easily lost, and can introduce malware into your systems. To reduce the likelihood of infection you can:
 - disable removable media using MDM settings
 - use antivirus tools where appropriate
 - only permit the use of sanctioned products
 - protect data at rest (encrypt) on removable media
 - encourage alternative means of file transfer (such as online tools).

Dr. Stephen Hill

137

New Zealand privacy watchdog John Edwards chosen as next information commissioner

Written by Sam Trendall on 26 August 2021 in News

Government chooses preferred candidate to replace Elizabeth Denham

Credit: Doc Searls/CC BY 2.0

The government has announced that New Zealand privacy commissioner John Edwards is set to become the UK's next information commissioner.

Edwards has been chosen as the preferred nominee for the regulatory role, which is set to be vacated in October when incumbent Elizabeth Denham ends her five-year stint in the hot seat. His appointment is subject to approval by the Digital, Media, Culture and Sport select committee.

Dr. Stephen Hill

138

Dr Stephen Hill

69


GDPR

Alex Hern
 @alexhern
 Thu 26 Aug 2021 10:19 BST

[f](#) [t](#) [e](#)

UK to overhaul privacy rules in post-Brexit departure from GDPR

Culture secretary says move could lead to an end to irritating cookie popups and consent requests online




▲ GDPR imposes strict restrictions on what data controllers can do with individuals' personal data Photograph: Alamy

Britain will attempt to move away from European data protection regulations as it overhauls its privacy rules after **Brexit**, the government has announced.

The freedom to chart its own course could lead to an end to irritating cookie popups and consent requests online, said the culture secretary, Oliver Dowden, as he called for rules based on "common sense, not box-ticking".

But any changes will be constrained by the need to offer a new regime that the EU deems adequate, otherwise data transfers between the UK and EU could be frozen.




AIB2021
virtual


Dr. Stephen Hill

139

Introducing Windows 11




Launch Date
October 5, 2021



AIB2021
virtual

Dr. Stephen Hill

140



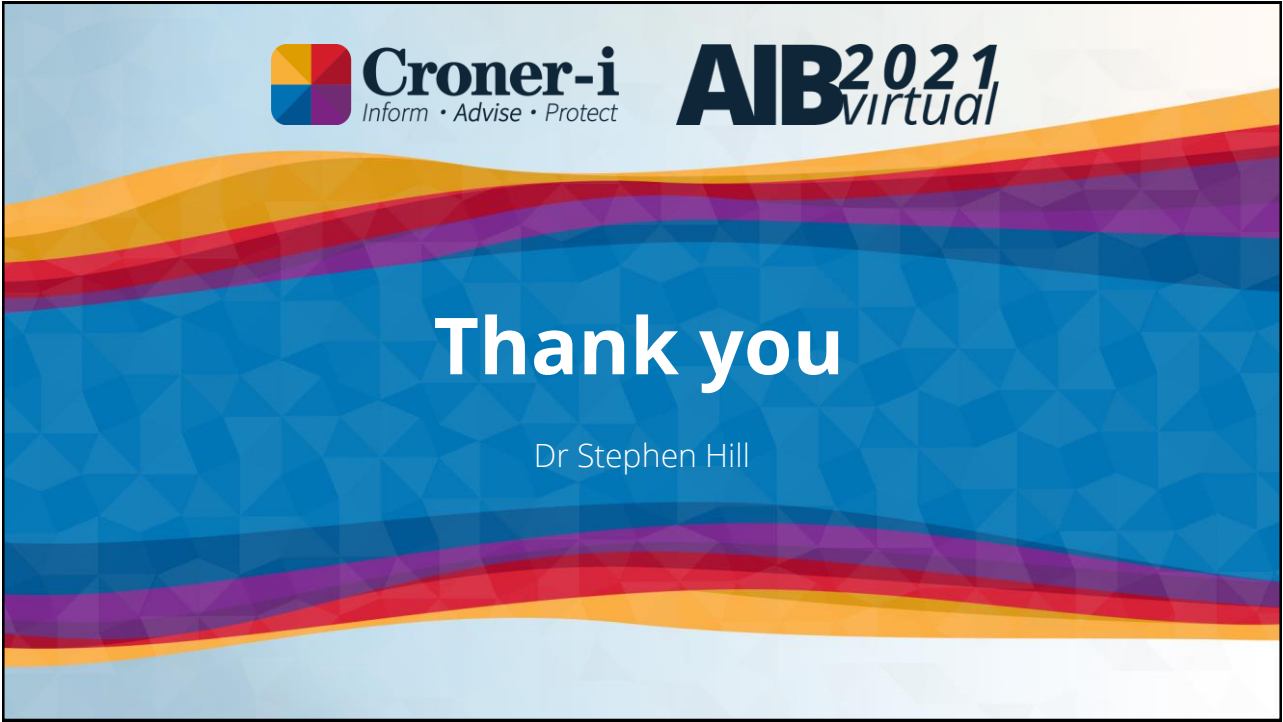
Office 2021 is not like Microsoft 365, which offers a cloud-based work experience

Office 2021 is a one-time purchase that provides Office programs for a single computer for a single upfront payment.

Croner-i *Inform • Advise • Protect* **AIB2021** *virtual*

Dr. Stephen Hill

141



Croner-i *Inform • Advise • Protect* **AIB2021** *virtual*

Thank you

Dr Stephen Hill

142