

Security Awareness Training Session



Nick Forster
SOC Manager

Agenda

- Current Threats & Tactics
- Email & Mobile Device Security
- Security Best Practices
- Discussion & Questions



ACSC Australian
Cyber Security
Centre

Current Threat Overview



**Repurpose Common
Tactics**



**Increase in Stolen
Passwords**



Phishing Analysis

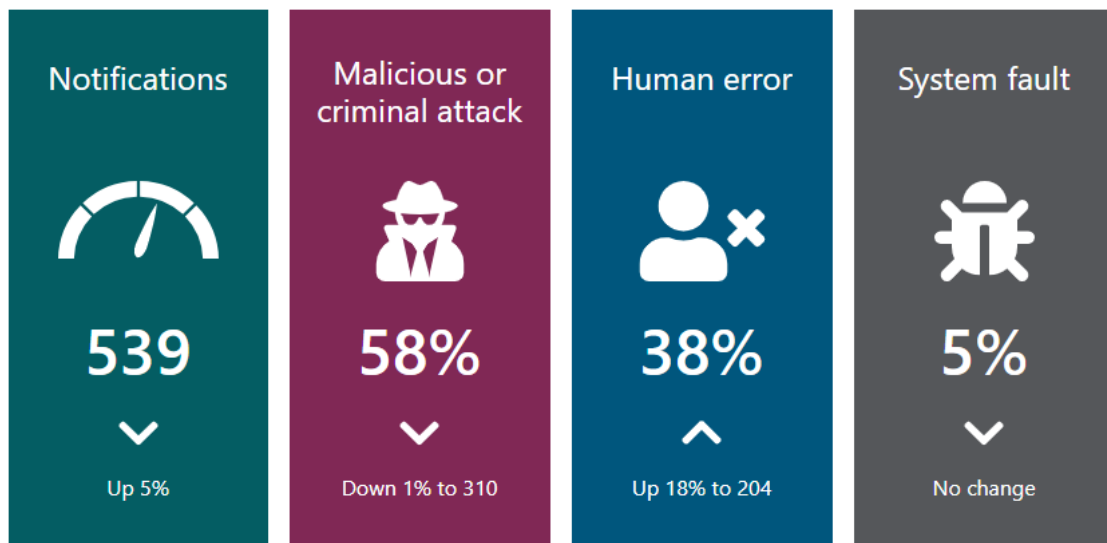


Increase in Human Error

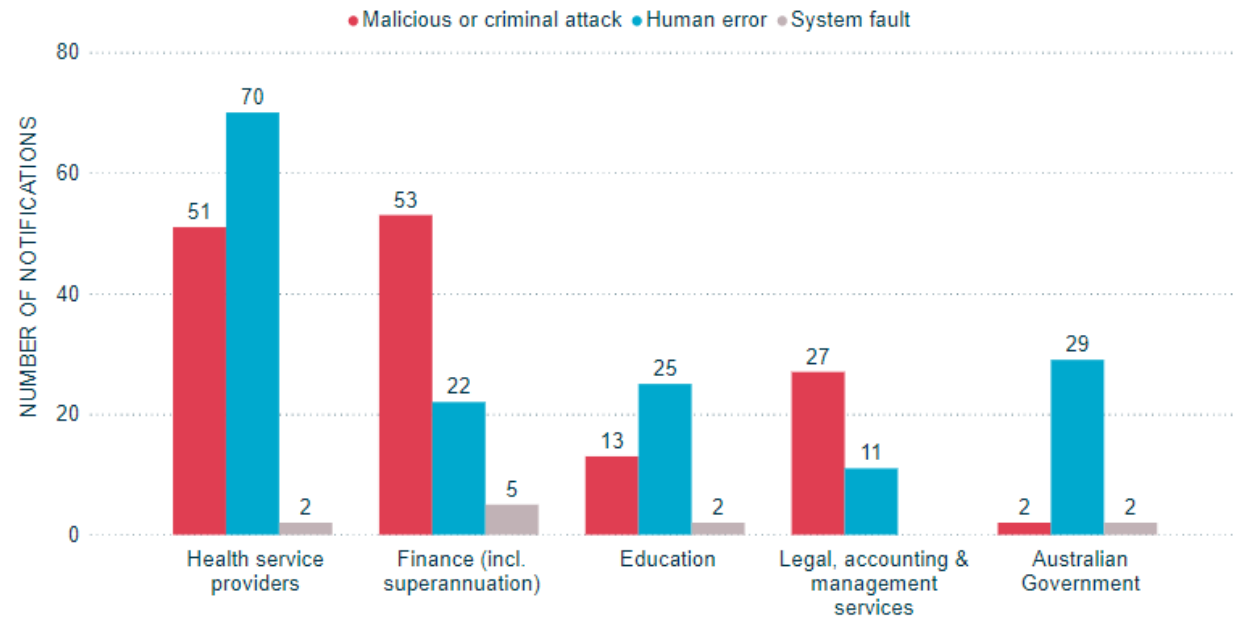


**Increase in
Ransomware**

OAIC Notifications



- *Office of the Australian Information Commissioner*
- *Notifiable Data Breach Scheme (Feb 2018)*
- *Bi-Annual Report (Jul 20 – Jan 21)*



Attack Methodology



Open-Source Intelligence



WiFi Exploitation



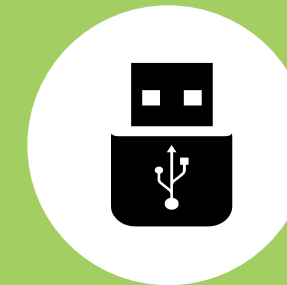
Social Media Exploitation



Spearphishing



Events



Device

How to Identify a Phish



How to Identify a Phish



Header

H-A-L-T In Action

From: E-mail Server <info@pacificairtransport.com>
Sent: Wednesday, 17 March 2021 10:25 am
To: [REDACTED]
Subject: Your mail-box is full

Mail-box is full

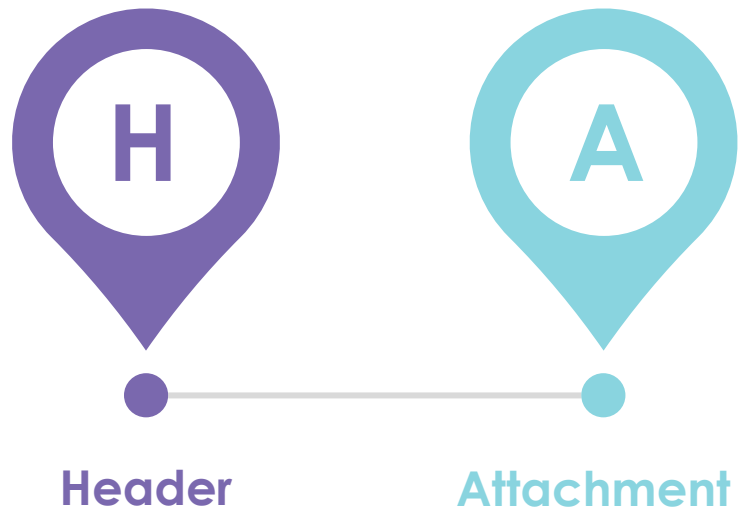
Your mailbox can no longer send or receive messages. update your storage

- Follow the link below to review them
- Update storage to continue receiving messages

[UPDATE STORAGE](#)


Best regards:

How to Identify a Phish



H-A-L-T In Action

From: ACCUEIL.DECHETS <accueil.dechets@perpignan-mediterranee.org>
Sent: Friday, 19 March 2021 3:22 pm
To: [REDACTED]
Subject: 19/03/2021 Settlement / Property Affairs - #B11402021

 FNTRACTS#11402021.pdf
42.6kb

Good Day,

Please also find attached our letter of today's date.

Please ensure you send through the documents requested as soon as possible so that we are not in breach.

Thank you

Kind Regards

Accueil Sonia Dechets

Principal Lawyer

PERPIGNAN-MEDITERRANEE

Suite 14/ 1 Elyard Street, Narellan NSW 2567
Phone 1800 675 304 | Fax 1800 993 426 |

E: Accueil@perpignan-mediterranee.com

**** Email Notification **** This e-mail is only intended for the person(s) to whom it is addressed and may contain confidential information. Unless



legal.platinum propertylaw.au sent you Platinum.pdf

"Kind Regards

Platinum Property Law."

You can download these files now or until **3/22/2021**.

Questions? Ask legal.platinum (legal.platinumpropertylaw.au@protonmail.com)

[Download files](#)

Here's what they sent you

1 item • 51 KB



Platinum.pdf

51.46 KB

How to Identify a Phish



H-A-L-T In Action

From: E-mail Server <info@pacificairstansport.com>
Sent: Wednesday, 17 March 2021 10:25 am
To: [REDACTED]
Subject: Your mail-box is full

Mail-box is full

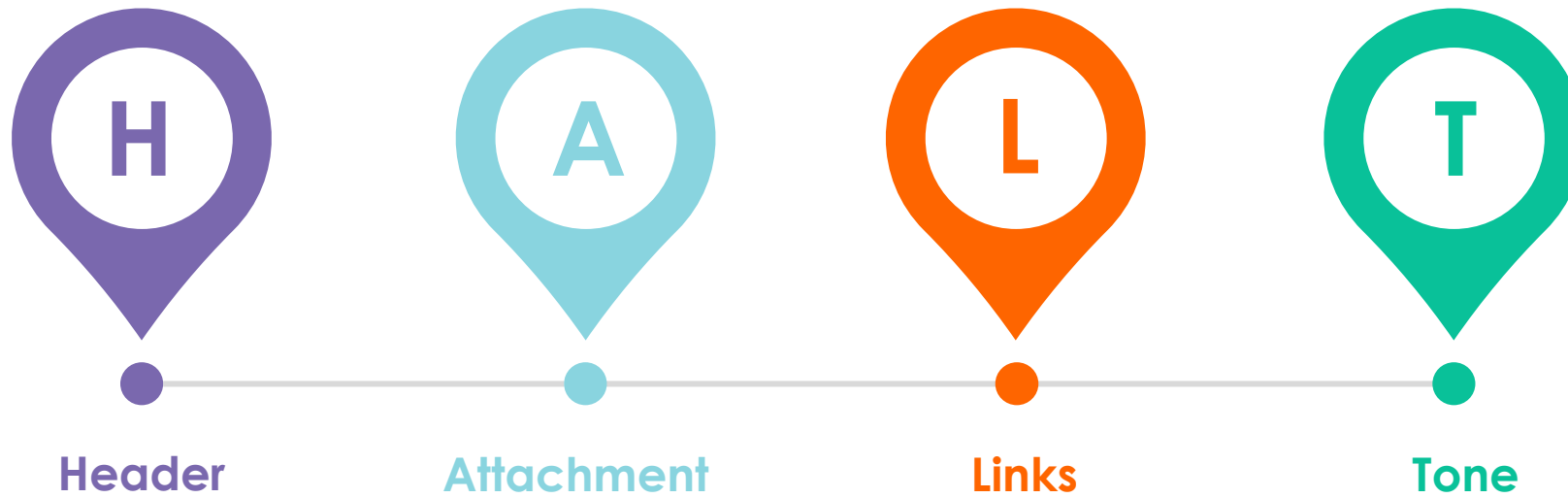
Your mailbox can no longer send or receive messages. update your storage

- Follow the link below to review them
- Update storage to continue receiving messages

[UPDATE STORAGE](#)

Best regards:

How to Identify a Phish



H-A-L-T In Action

From: office-desk@officelinesvii.com [mailto:office-desk@officelinesvii.com]
Sent: Friday, 5 March 2021 10:51 am
To: [REDACTED]
Subject: New DD

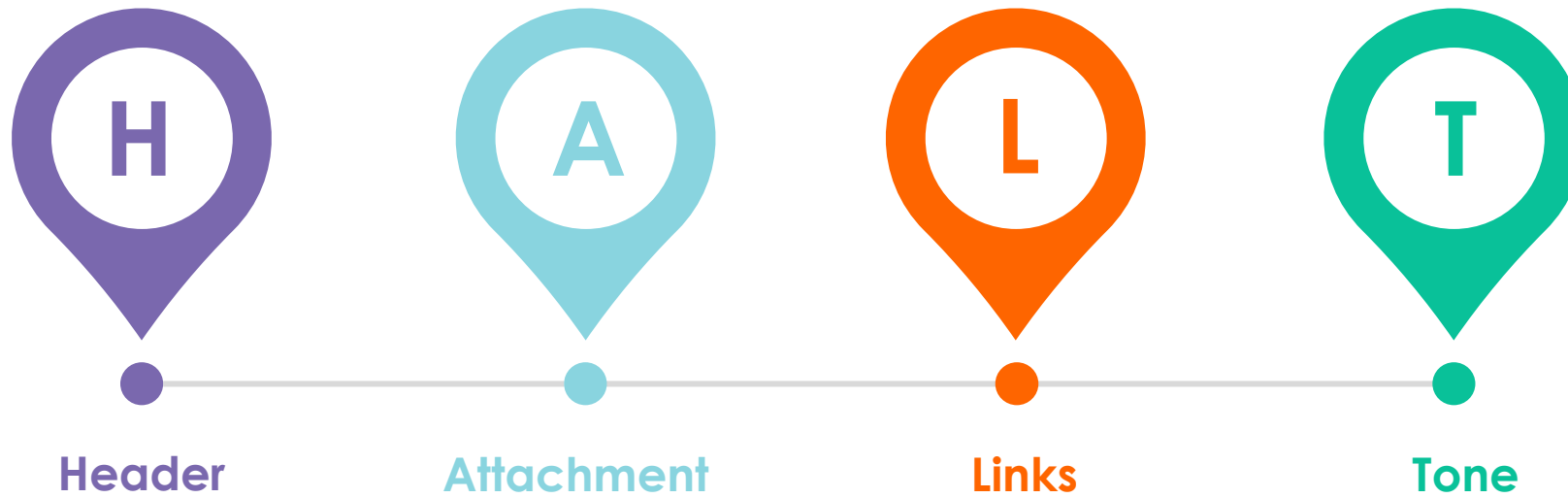
Julia,

I would like to have my payroll/benefits of direct deposit changed to my new details. The previous account on file will be inactive in 5 days. I need your immediate assistance on this matter.

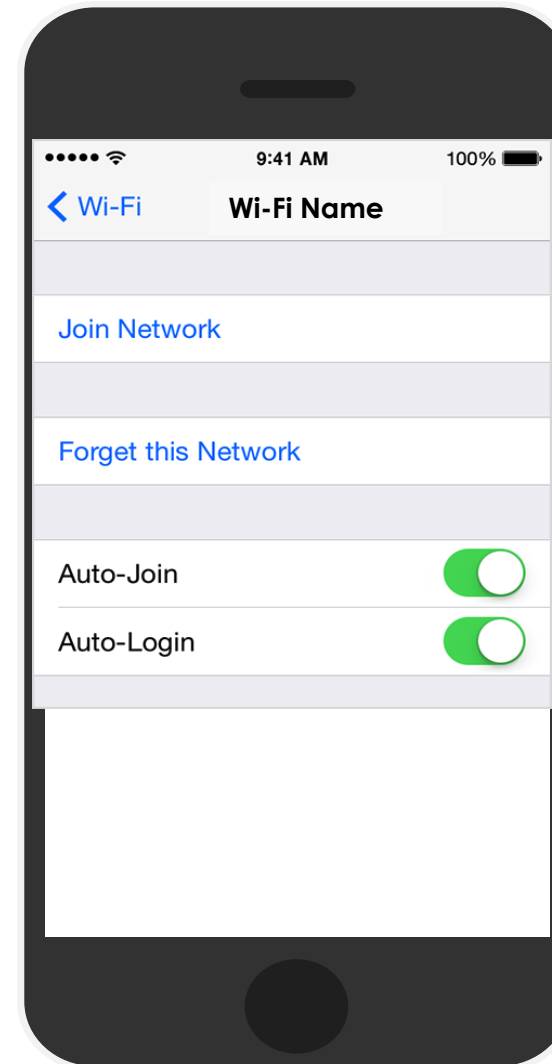
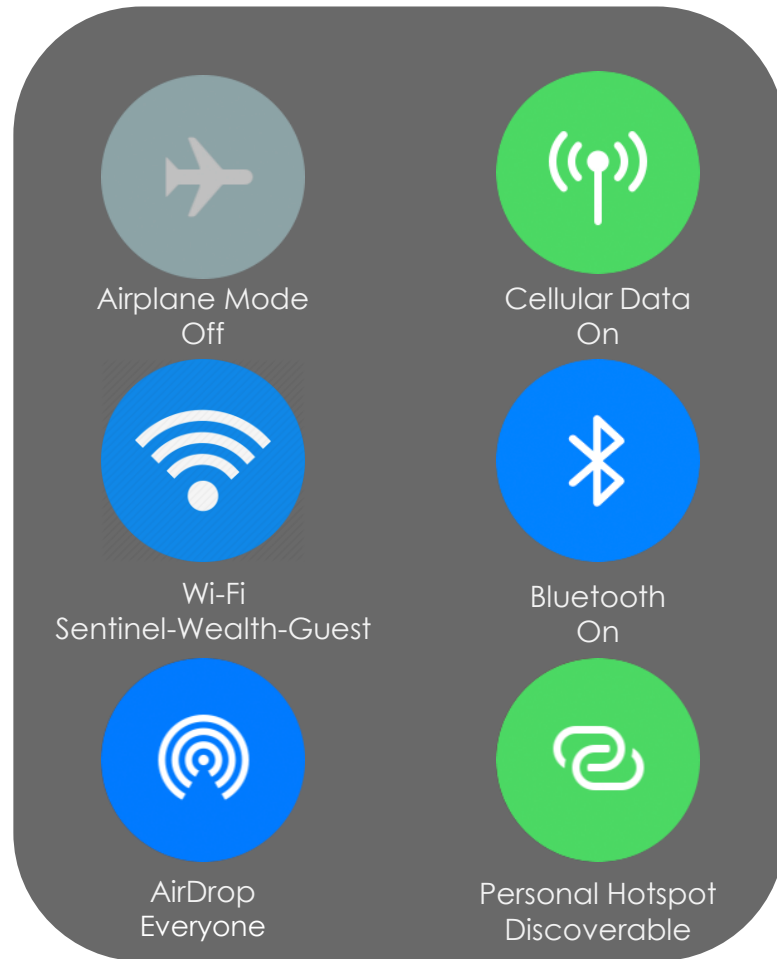
Regards,

[REDACTED]

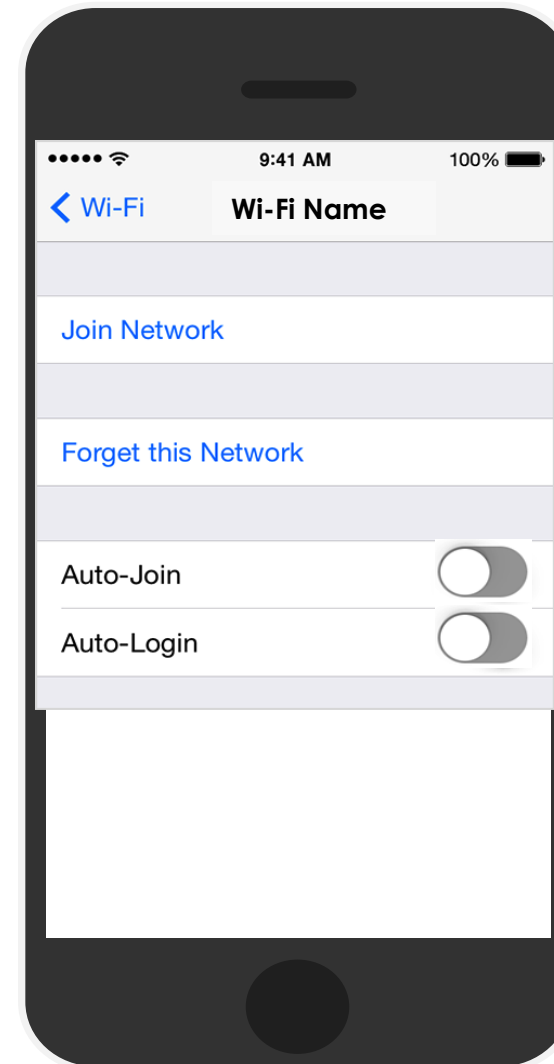
How to Identify a Phish



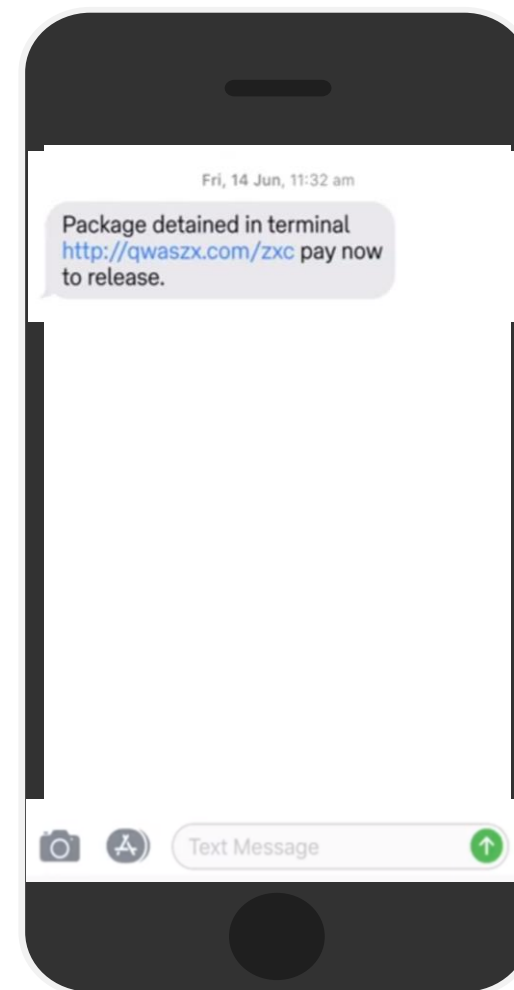
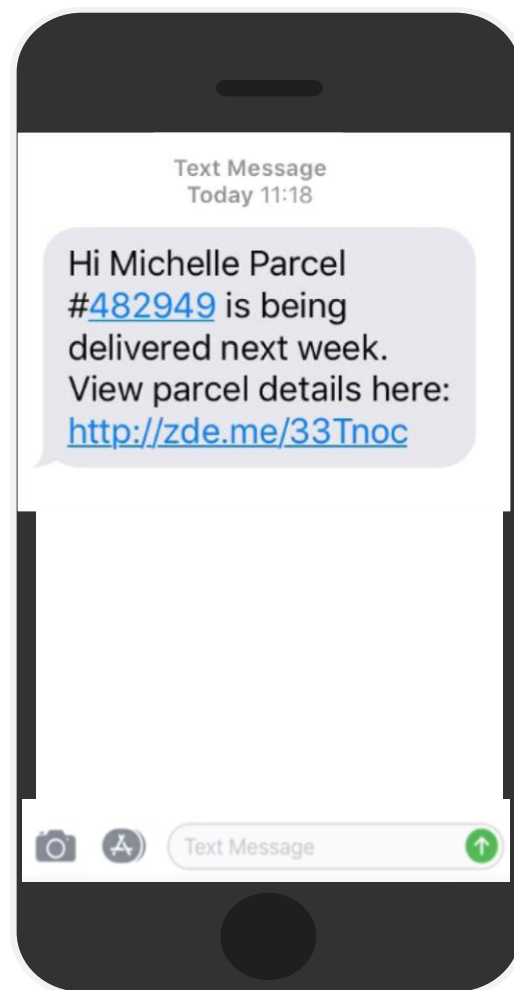
Mobile Security Awareness - Apple



Mobile Security Awareness - Apple



Mobile Security Awareness - SMSishing




Social Media and Privacy Settings


Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)


3 Steps to better security [Start using 1Password.com](#)



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.




Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

[f](#) [t](#) [b](#) [p](#) Donate


Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames



Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles



Physical Security

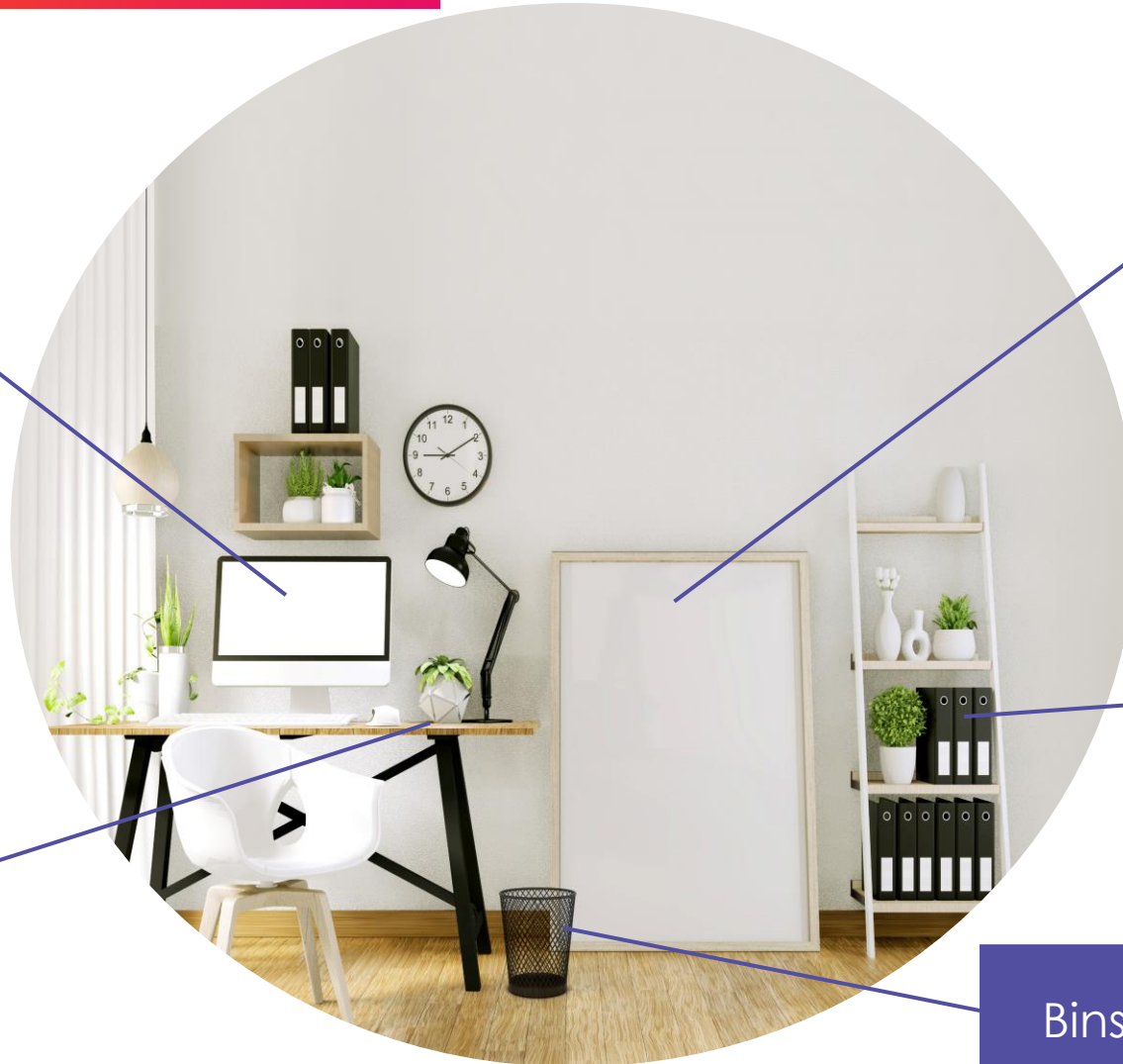
Screen
Lock

Post-Its

Documents

Storage
Devices

Bins



The Most Common Passwords of 2020

- **WINNER: “123456”**
- **Less than a second to crack**
- **Exposed over 23 million times this year**

1	123456	21	123	41	evite	61	123654	81	asd123	101	jordan	121	hunter	141	anthony	161	456789	181	b123456
2	123456789	22	omgpop	42	123abc	62	ohmnamah23	82	555555	102	anhyeuem	122	686584	142	yugioh	162	azerty	182	whatever
3	picture1	23	123321	43	123qwe	63	12345678910	83	a123456789	103	killer	123	iloveyou1	143	fuckyou1	163	andrea	183	welcome
4	password	24	654321	44	sunshine	64	zing	84	888888	104	basketball	124	987654321	144	amanda	164	q1w2e3r4	184	ginger
5	12345678	25	qwertyuiop	45	121212	65	shadow	85	7777777	105	michelle	125	justin	145	asdf1234	165	qwer1234	185	flower
6	111111	26	qwer123456	46	dragon	66	102030	86	fuckyou	106	1q2w3e	126	cookie	146	trustno1	166	hello123	186	333333
7	123123	27	123456a	47	1q2w3e4r	67	11111111	87	1234qwer	107	lol123	127	hello	147	butterfly	167	10203	187	111111111
8	12345	28	a123456	48	5201314	68	asdfgh	88	superman	108	qwerty1	128	blink182	148	x4ivygA51F	168	matthew	188	robert
9	1234567890	29	666666	49	159753	69	147258369	89	147258	109	789456	129	andrew	149	iloveu	169	pepper	189	samsung
10	senha	30	asdfghjkl	50	0123456789	70	qazwsx	90	999999	110	6655321	130	25251325	150	batman	170	12345a	190	a12345
11	1234567	31	ashley	51	pokemon	71	qwe123	91	159357	111	nicole	131	love	151	starwars	171	letmein	191	loveme
12	qwerty	32	987654321	52	qwerty123	72	michael	92	love123	112	naruto	132	987654	152	summer	172	joshua	192	gabriel
13	abc123	33	unknown	53	Bangbang123	73	football	93	tigger	113	master	133	bailey	153	michael1	173	131313	193	alexander
14	Million2	34	zxcvbnm	54	jobandtalent	74	baseball	94	purple	114	chocolate	134	princess1	154	00000000	174	123456b	194	cheese
15	000000	35	112233	55	monkey	75	1q2w3e4r5t	95	samantha	115	maggie	135	123456	155	lovely	175	madison	195	passw0rd
16	1234	36	chatbooks	56	1qaz2wsx	76	party	96	charlie	116	computer	136	101010	156	jakcgt333	176	Sample123	196	142536
17	iloveyou	37	20100728	57	abcd1234	77	daniel	97	babygirl	117	hannah	137	12341234	157	buster	177	777777	197	peanut
18	aaron431	38	123123123	58	default	78	asdasd	98	88888888	118	jessica	138	a801016	158	jennifer	178	football1	198	11223344
19	password1	39	princess	59	aaaaaa	79	222222	99	jordan23	119	123456789a	139	1111	159	babygirl1	179	jesus1	199	thomas
20	qqww1122	40	jacket025	60	soccer	80	myspace1	100	789456123	120	password123	140	1111111	160	family	180	taylor	200	angel1

Password Best Practices

Composition:

- Minimum of 8 characters or more
- No sequences
- No patterns
- No PII!

Three of the following categories:

- Uppercase (A through Z)
- Lowercase (a through z)
- Numbers (0 through 9)
- Special characters: (~!@*)

Consider Easy to remember random Passphrases such as:

65 - Helicopter - * -
cup - Tree =
65Helicopter*cupTree

Passphrases

Discussion

- W4t3Rme!On_nb
- GodSaveTheQueen2021*241187
- @soap483DRUM

Reporting & Immediate Actions

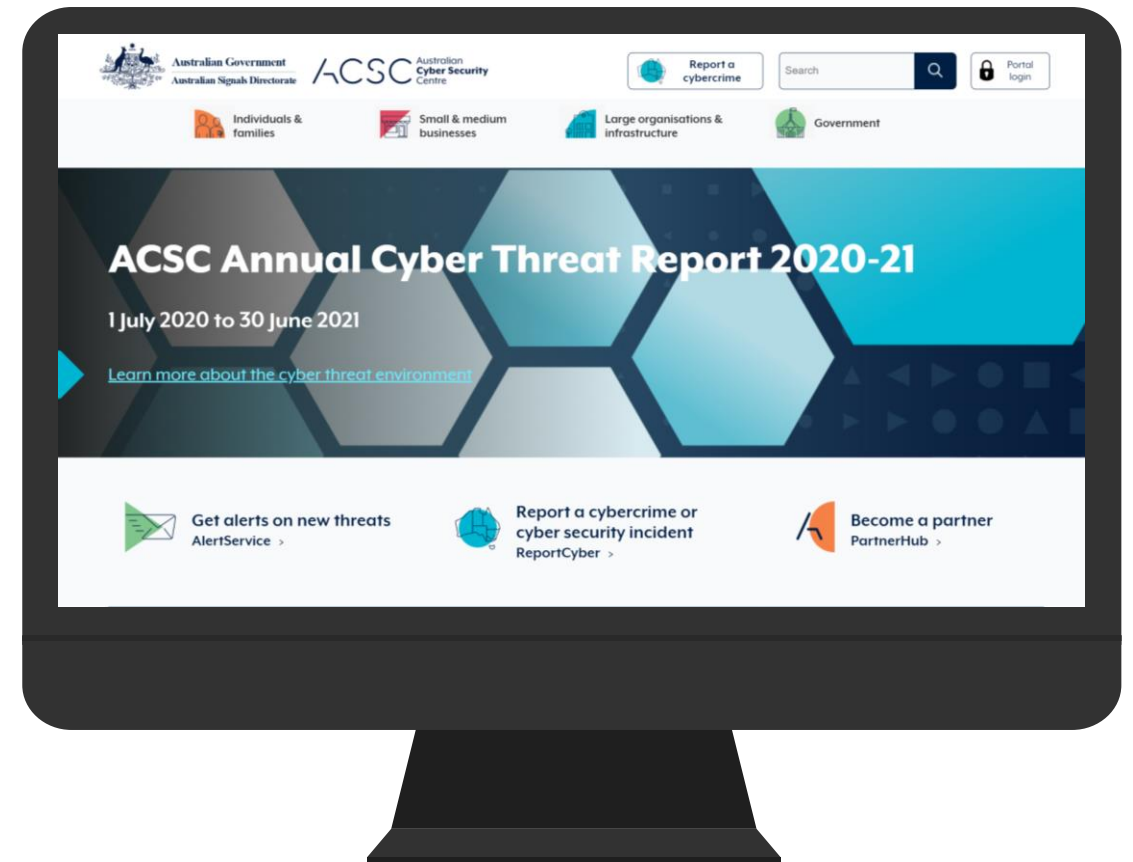
Should you suspect that your computer is infected, take immediate action:

- **Don't Panic**
- Document what you did and saw
- Disconnect from the Network and Internet
- Contact the ACSC Cyber Hotline or the Police

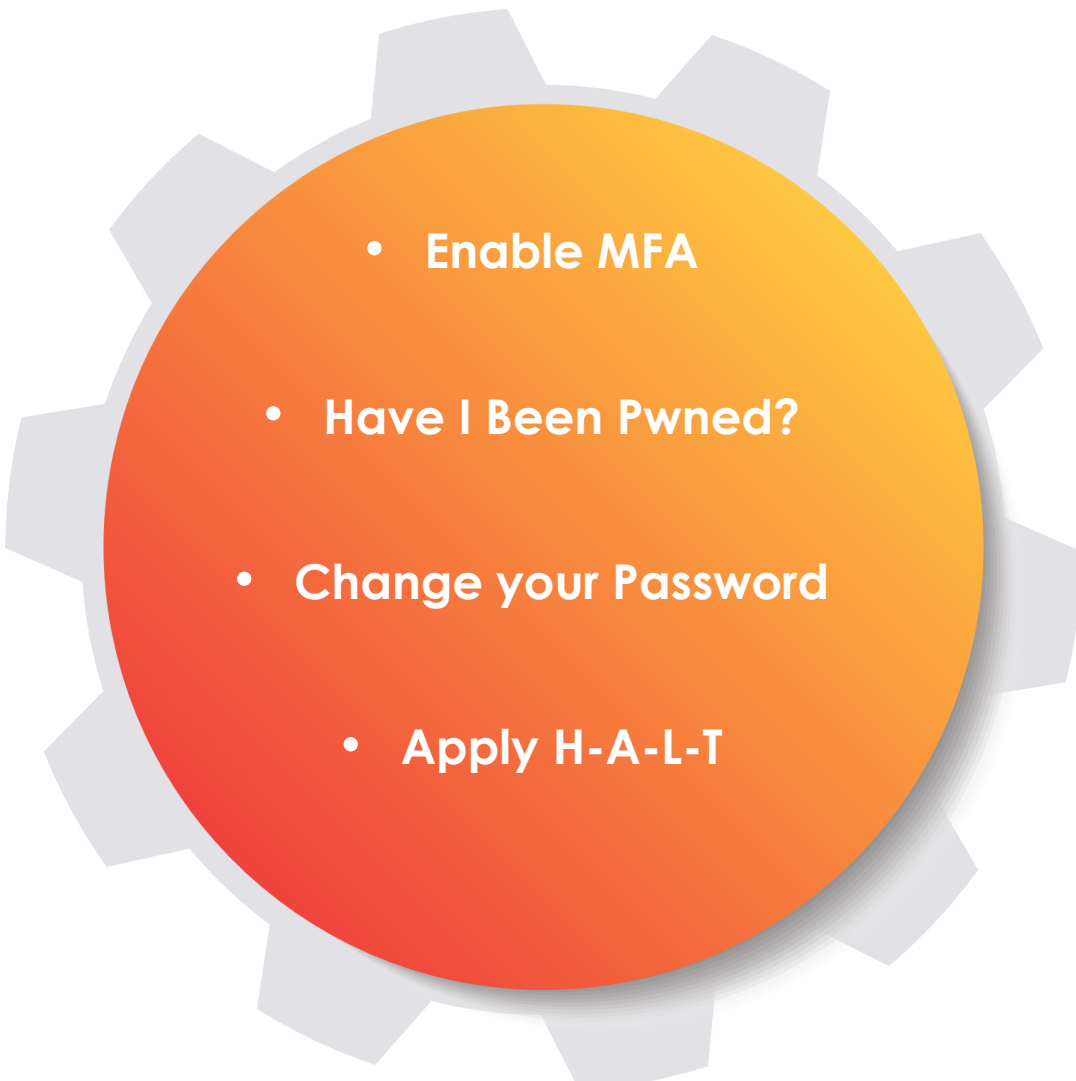
Emergency: 000

ACSC Cyber Hotline:

<https://reportapp.cyber.gov.au/#/person>



Next Steps...

- 
- Enable MFA
 - Have I Been Pwned?
 - Change your Password
 - Apply H-A-L-T







Q&A

Thank you

