Preventing Account Takeover by Cyber Criminals

itconnexion

Poll

itconnexion

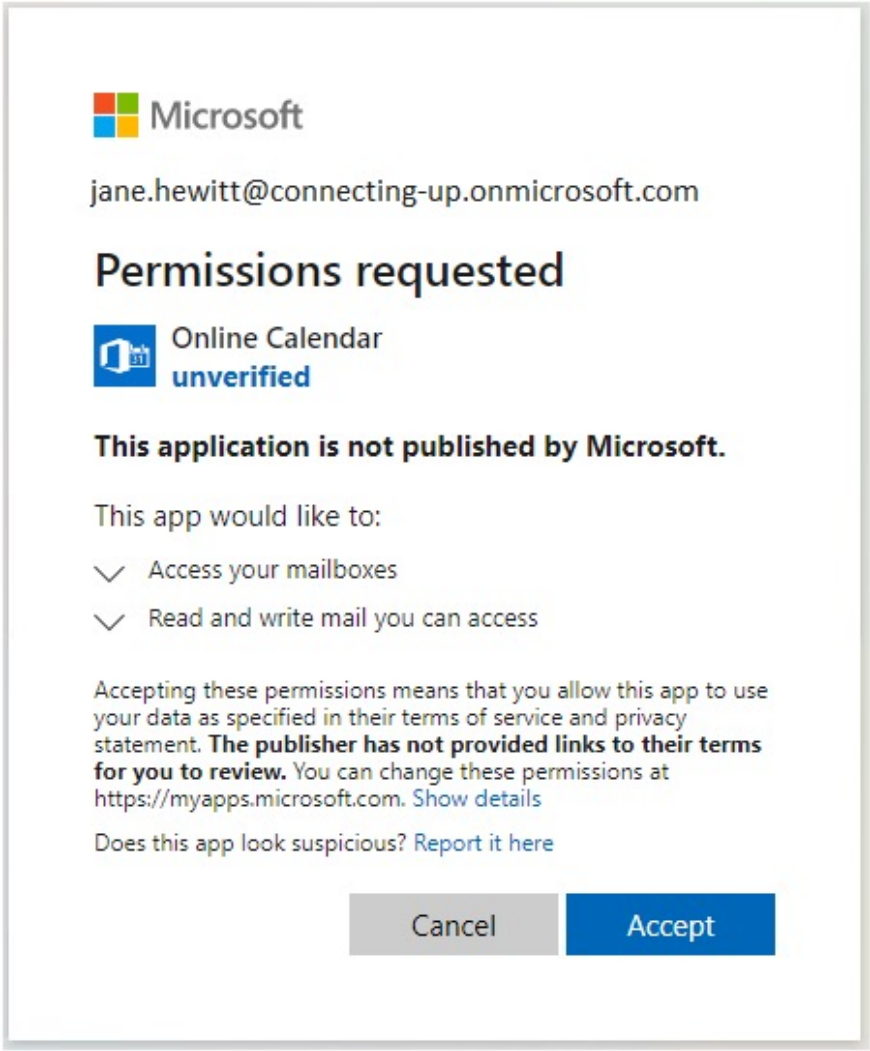
Have you received phishing email in the last 3 months?

- Yes
- Maybe
- No, we have robust anti-spam platform

Poll

Would you accept the invite?

- **Yes**
- **Maybe**
- **No**



Evolving threat landscape

DarkSide ransomware gang, Aug 2020 – May 2021

Structured organisation championing RaaS (Ransomware as a Service) with principles and organisation vision:

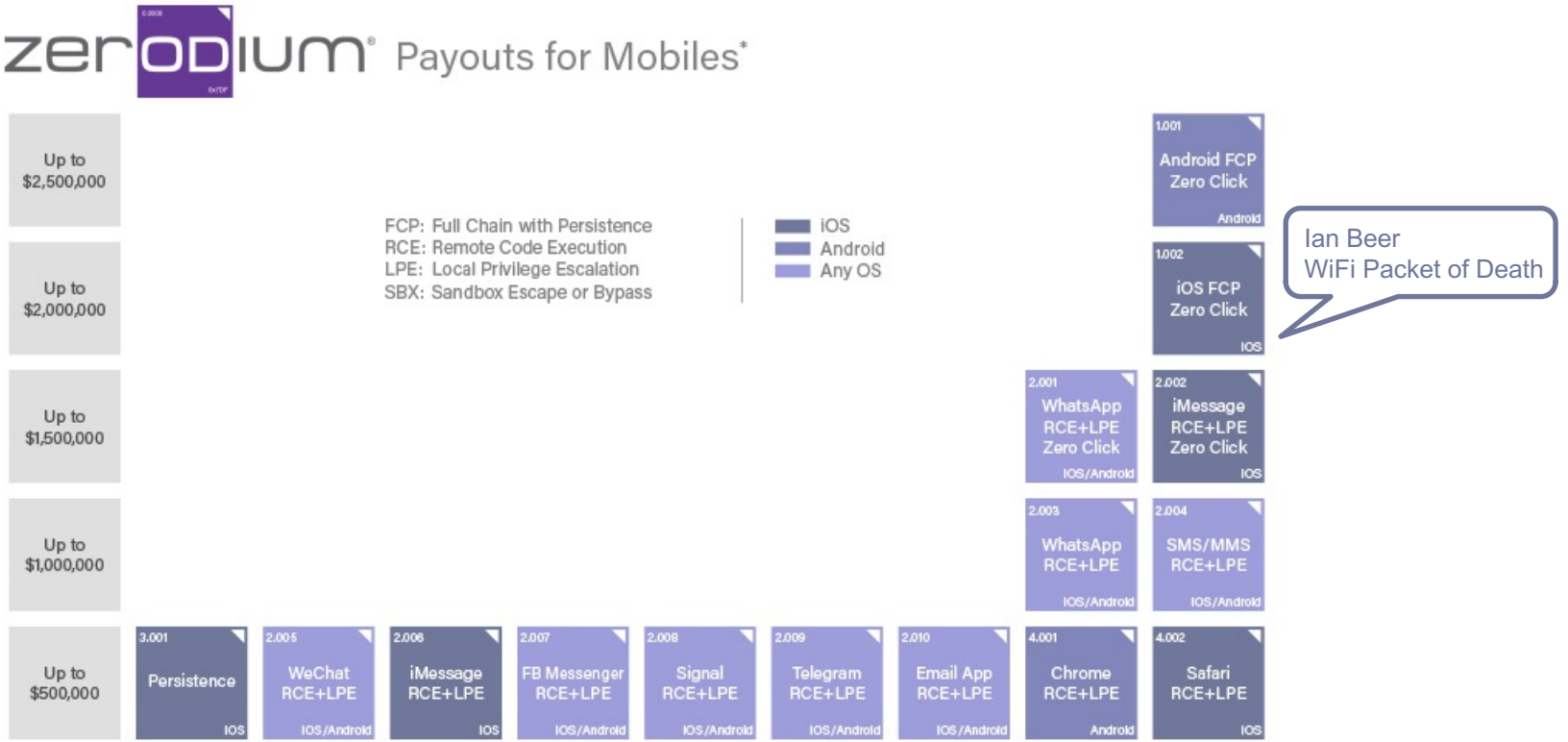
- Selective target: no health/education/govt sector, no NFP, no critical infrastructure. Only large profitable enterprise, with carefully calculated ransom amount derived from analysing financial statements.
- Donates to charity $10,000USD to 2 charities via The Giving Block
- Provide guarantee of one file decryption to assure authenticity, offer technical support to assist with decryption and not posting leak on public web.

On 6 May '21, DarkSide is credited to be responsible for Colonial Pipeline shutdown over 6 days, stopping approx. 45% of oil supply in Eastern Seaboard / US East Coast region. Emergency of this magnitude has potential significant impact on US economy as fuel prices spike and fluctuating oil share prices.

On 14 May '21, DarkSide ceased operation, releasing all cryptokeys as their servers were seized and their crypto funds diverted to another account, "at the request of law enforcement agencies".

Other cyber criminal groups using RaaS model: REvil/Sodinokibi, Ryuk, Lockbit, Egregor/Maze.

Case Study


zerodium Payouts for Mobiles*
Up to $2,500,000
Up to $2,000,000
Up to $1,500,000
Up to $1,000,000
Up to $500,000
FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
iOS
Android
Any OS
1.001 Android FCP Zero Click Android
1.002 iOS FCP Zero Click iOS
Ian Beer
WiFi Packet of Death
2.001 WhatsApp RCE+LPE Zero Click iOS/Android
2.002 iMessage RCE+LPE Zero Click iOS
2.003 WhatsApp RCE+LPE iOS/Android
2.004 SMS/MMS RCE+LPE iOS/Android
3.001 Persistence iOS
2.005 WeChat RCE+LPE iOS/Android
2.006 iMessage RCE+LPE iOS
2.007 FB Messenger RCE+LPE iOS/Android
2.008 Signal RCE+LPE iOS/Android
2.009 Telegram RCE+LPE iOS/Android
2.010 Email App RCE+LPE iOS/Android
4.001 Chrome RCE+LPE Android
4.002 Safari RCE+LPE iOS

In Australia

Cyber crime is a growing industry globally

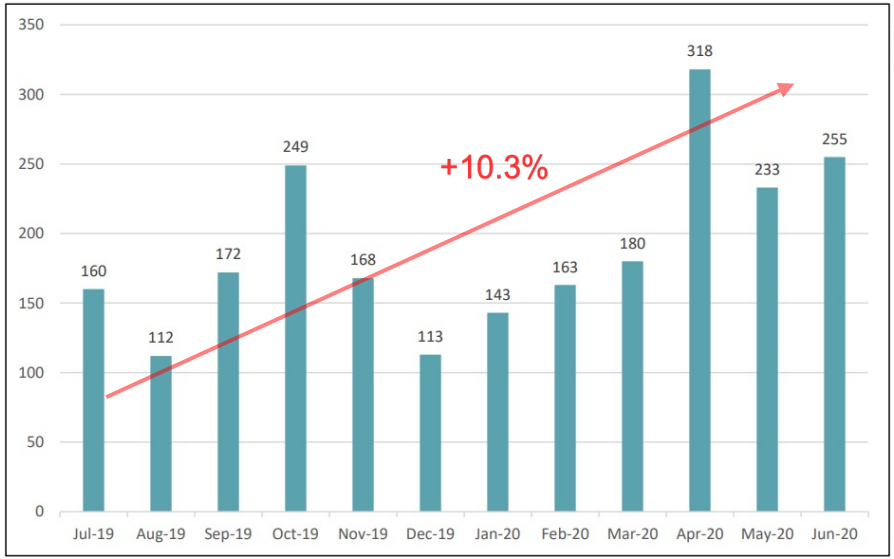
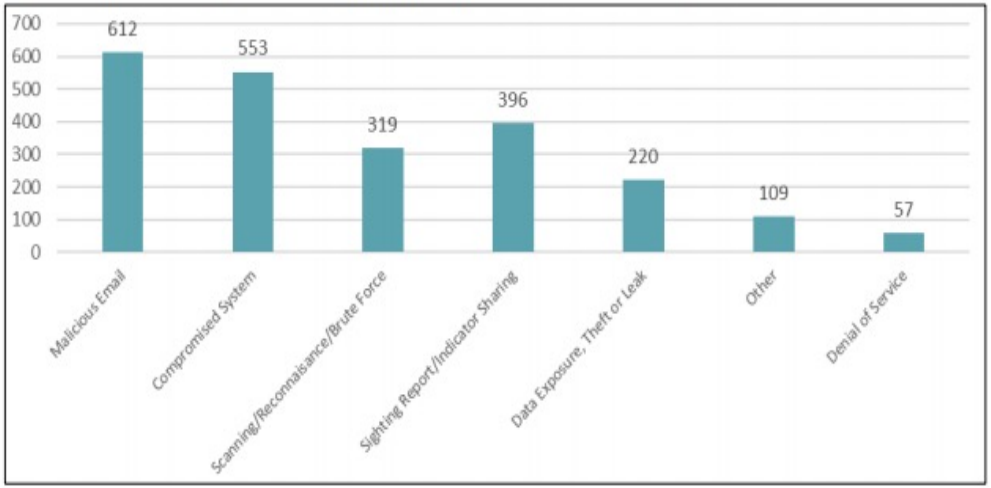


Figure 4: Cyber security incidents, by type (1 July 2019 to 30 June 2020)



**ACSC Annual Cyber Threat Report '19-'20*

Data Breach Examples

- LinkedIn – 2016
- FPNSW – 2018
- Page Up People – 2018
- Melbourne Polytechnic TAFE - 2018
- Canva – 2019
- Spotify - 2020
- Zoom – 2020
- Scouts Victoria – 2020
- AFL - 2020
- Optus - 2020
- Eastern Health (Cabrini Health) - 2021

Many of these data leaks are publicly available on the dark web for free, although initially, access is paywalled on data leak forums.

Eventually compiled into one big database, called COMB (Compilation Of Many Breaches).

These data leaks can also be cross referenced to create target profile.

Password Re-use

itconnexion

Multi Factor Authentication

Poll

itconnexion

Do you implement Multi Factor Authentication in your organisation?

- Yes, policy enforced for all
- Yes, for some accounts
- No

Business Email Compromise

itconnexion

- Client A
  - Email account compromised due to credential theft via email phishing link.
  - Attacker access O365 account and hijacks email conversation.
  - Using hijacked email, attacker 'authorises' $30,000 payment for an invoice to financial controller.

From: Your Boss <yourboss@fakeyourcompany.com>
Sent: 09 October 2018 11:06
To: Your Company Finance <finance@yourcompany.com>
Subject: IMPORTANT: Fund Transfer Done Today

Hi Gwen,

Could you do me a favour? There's a pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me because I can't access the accounts from here.
They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked!)
Just click on the link in their email and transfer the amount to the account they specify.

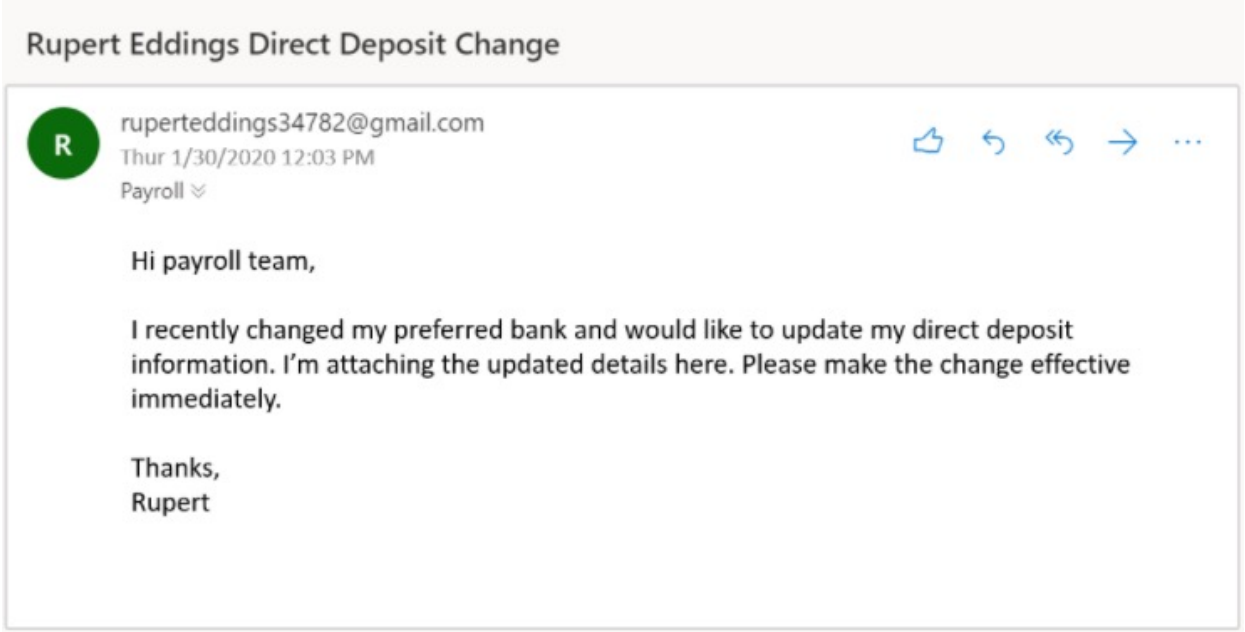
This needs to be done TODAY so make it high priority.

If you do this for me it would be a huge favour.

Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,
Your Boss

Payment Redirection



- Verification procedure for change of financial detail from debtors, to creditors?
- Simple phone call verification.
- Cyber security insurance policy.
- Continuous phishing training.

Payment Redirection

itconnexion

```
Received: from SYBPR01MB3706.ausprd01.prod.outlook.com
 ([fe80::a031:c345:7438:33d0]) by SYBPR01MB3706.ausprd01.prod.outlook.com
 ([fe80::a031:c345:7438:33d0%5]) with mapi id 15.20.4242.023; Tue, 22 Jun 2021
 06:13:53 +0000
From: John Doe <JohnDoe@contoso.com.au>
To: Homer Samson <hsamson@juiceshop.com>
Subject: Bank Change [SEC=OFFICIAL]
Thread-Topic: Bank Change [SEC=OFFICIAL]
Thread-Index: AddnL456iG7/qM2ehLnFw==
Date: Tue, 22 Jun 2021 06:13:53 +0000
Message-ID:
 <PR01MB370636B7EB00F73AC9E44976C5099@PR01MB3706.ausprd01.prod.outlook.com>
Accept-Language: en-AU, en-US
Content-Language: en-US
received-spf: Pass (protection.outlook.com: domain of contoso.com.au designates
 1.2.3.4 as permitted sender) receiver=protection.outlook.com;
 client-ip=1.2.3.4; helo=data.net.au;
authentication-results: spf=pass (sender IP is 1.2.3.4)
 smtp.mailfrom=contoso.com.au; juiceshop.com; dkim=pass (signature was verified)
 header.d=contoso.com.au;juiceshop.com; dmarc=pass action=none
 header.from=contoso.com.au;compauth=pass reason=100
x-originating-ip: [4.3.2.1]
[SNIP]
x-forefront-antispam-report:
 CIP:1.2.3.4;CTRY:AU;LANG:en;SCL:1;SRV:;IPV:NLI;SFV:NSPM;H:data.net.au;PTR:data.ne
 3)(55016002)(7596003)(7636003)(9686003)(86362001)(6916009)(33656002)(8636004)(109
```

Payment Redirection is difficult to detect because email is sent from legitimate source as account was compromised.

- Original MTA source comes from genuine Microsoft as seen in prod.outlook.com subdomain.
- SPF/DKIM/DMARC will pass validation if sender organisation has set them up correctly.
- Microsoft has analysed the email and concluded it's not spam or malicious email.

Poll

Confidence rate in defending against phishing attack:

- **100%. No one in my company will fall for phishing attack.**
- **70%, I know some people will get phished.**
- **I've not done an assessment to understand my staff risk.**
- **We have continuous phishing training.**

Impact on NFPs

What does this all mean for NFPs? What we know:

- Shift to RaaS model:
  - Expert developers focus their time on producing more accurate and stable exploits.
  - Skill barriers to entry is much lower, as affiliates can purchase malware products and click a button to start an attack which means the number of attacks will increase.

- Damage from system compromise is several:
  - Client Privacy – Breach of Probity clause (DFFH Service Agreement or DHHS obligations).
  - Reputational – Loss of client/customers, fundraising capability.
  - Financial – Loss of funding/grants, fraudulent bank transfer.
  - Legal – Halt of operation from cyber investigation, possibly lawsuit from data breach ($1,000 - $20,000 per individual)

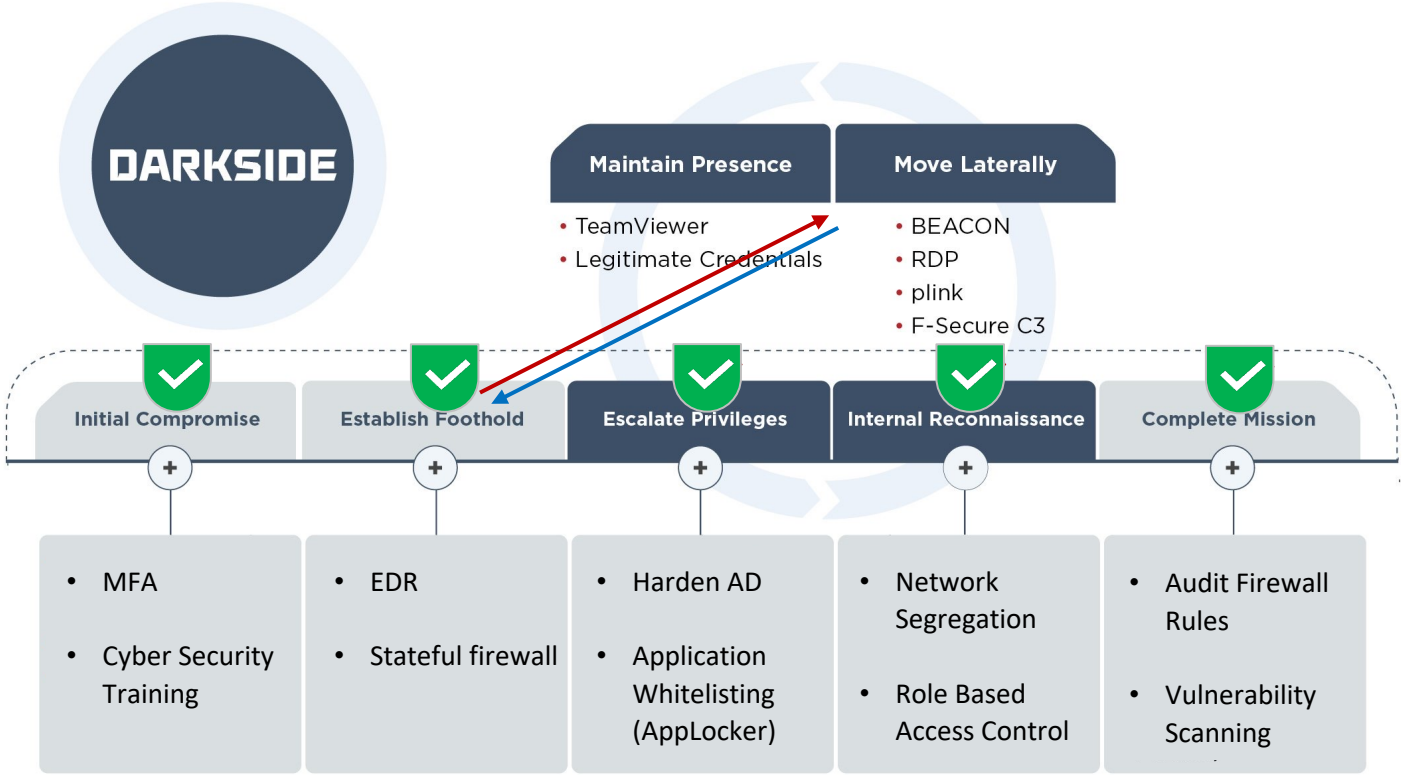
- Threat will persist long in the future; NFPs need to take action to strengthen their cyber security posture no matter how small the organisation size.

MITRE ATT&CK

Adversarial **T**actics, **T**echniques, **& C**ommon **K**nowledge

Framework that describes an attack chain process based on real-world observations.

Mitigation Strategies



*FireEye DarkSide Threat Research

itconnexion

Cyber Security Awareness Training (CSAT) Program 2021

- Fully funded by AusGov, no cost to NFPs
- Customised white-hat phishing campaigns
- Weekly consultation and monthly statistical reports

Click here to REGISTER

Please contact us for more information
1800-892-200 or info@itconnexion.com

Australian Government
Department of Industry, Science, Energy and Resources

This project is funded by the Australian Government Department of Industry, Science, Energy and Resources through the Cyber Security Business Connect and Protect Program.

itconnexion

Australian Government

Department of Industry, Science, Energy and Resources

This project is funded by the Australian Government Department of Industry, Science, Energy and Resources through the Cyber Security Business Connect and Protect Program.

In the spirit of reconciliation, ITConnexion Pty Ltd acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

Cyber Security Training Program

01 Provide access to online cyber security awareness training modules for the organisations' employees

02 White-hat phishing campaigns which will simulate realistic and challenging phishing attacks customised to the organisation industry/sector and localised to their area to increase the relevance, which includes:

- Managed simulated phishing campaigns
- Personalized training for end users caught in a simulated attack Progress reporting on phishing and training results

03 Consultation to discuss the training result and other cyber-risk

04 A webinar to educate Executives and key Stakeholders on cyber-risk mitigation strategies

Program Delivery & Schedule

Program Stage	Activities	Duration	Participant
Acceptance Stage	Program Briefing NDA & Agreement Information Gathering	1 week approximately	ITConnexion, Client's Executive
Onboarding Stage	Training Campaign Setup	1 week approximately	ITConnexion
Employees Training Stage	Online Training Portal Phishing Campaign Weekly follow-ups and progress report	8 Weeks	ITConnexion, Client's Employees, Client's Executive
Executive Training Stage	Final Report & Discussion Client to complete Australian Government Cyber Security Assessment Tool	2 days approximately	ITConnexion, Client's Executive
Wrap-Up Stage	CSAT Program Executive Webinar Client Survey & Feedback Form Follow-ups Discussions	2 days approximately	ITConnexion, Client's Executive

About ITConnexion

ITConnexion (founded in 2003) is a next-gen IT MSP operating in 10 cities and 2 countries with approximately 50 employees.

We provide the technology advice, solutions, and services around ICT support, infrastructure, cloud, cyber-security, and software development (mobile/web apps, SharePoint, Dynamics, PowerBI, etc.)

We have a strong client base in the NFPs, Government Agencies, and Peak Body Associations sectors; and a growing base of professional services, research and education institutions, healthcare, and multinational finance companies.

40+	160+	10+	2	200+	2300+	3800+
Team of IT Experts	Companies Supported	Cities Location	Countries Presence	Servers Managed	PCs Managed	IT Users Supported

Partnership

ITConnexion partners with world-leading technology vendors to give our clients access to the best technologies and innovative solutions that they can use to address their business challenge.

We train our team to master these chosen technologies so we can help our clients extract the maximum value of their technology investment.

We have strong partnership level with leading technology providers, such as Microsoft Gold Partner, Sophos Gold Partner, Datto Premier Partner, HP Enterprise Partner, and Accredited Digital Seller for the Australian Government

Microsoft Partner
Microsoft
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions
Gold DataCenter
Silver Collaboration and Content

datto
PARTNER PLUS
Premier
PARTNER

Australian Government
Digital Marketplace
Accredited Seller

SOPHOS
Gold Partner

vmware PARTNER
PROFESSIONAL SOLUTION PROVIDER

vmware PARTNER
ENTERPRISE SOLUTION PROVIDER

veeam
CLOUD & SERVICE PROVIDER
SILVER

hp
Hewlett Packard Enterprise

Questions?

2 / 22 Gillman Street Hawthorn East VIC 3123
1300 89 22 00 | contactus@itconnexion.com | **www.itconnexion.com**