

Digital Security Workshop Email

March 2025

Contents

- Introduction
- Cyber Landscape
- Protecting Email
- Securing Cloud Email
- Protecting Against Compromised Accounts
- DMARC
- Blacklisting and Breaches
- Email from Devices and Software
- Visibility
- Final Thoughts
- Discussion

Introduction

Who am I

- John King
 - 021476622
 - john.king@thinking.net.nz
- 39 years in IT, 32 in Cyber Security

Who are we and what do we do

- Cyber Security and Managed Services Provider
- NZ and Australia predominant
- Purple Team
 - Simultaneously test and defend the organization and its assets
 - To improve the overall security posture and preserve the health of the organization over both the short- and long-term
- Specialise in OT (operational technology), Cloud and Identity
 - Email
 - Authentication
 - Cloud Migration

What are we discussing today

- Protecting against spam, phishing and malware
 - Protecting against compromised accounts
 - Verifying that email is legitimate
- How to check for blacklisting of my email and exposure to public breaches
- Dealing with photocopiers, printers, other software and similar products
- Reporting for visibility

Cyber Landscape

Threat Intelligence Summary

- An organization in New Zealand is being attacked on average 1489 times per week in the last 6 months.
- The top malware in New Zealand is FakeUpdates.
- The top malware list in New Zealand includes 4 Botnets, 1 Mobile (Anubis), 1 RAT (Remcos), 1 Infostealer (Anubis) and 1 Downloader (FakeUpdates).
- The most common vulnerability exploit type in New Zealand is Information Disclosure, impacting 55% of the organizations.
- Weekly impacted organizations by malware types:

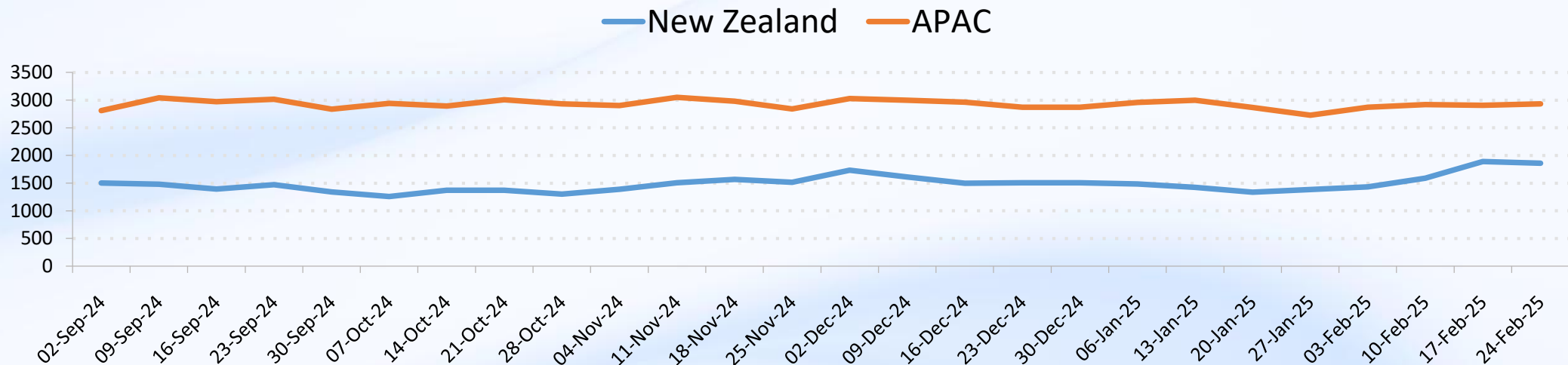
	Ransomware	Mobile	InfoStealer	Banking	Botnet
New Zealand Avg.	2.1%	0.2%	0.7%	0.7%	4.2%
APAC Avg.	4.5%	1.1%	5.2%	3.9%	11.1%

Threat Landscape

- **Cyber Wars** – Nation-states are leveraging AI-driven tactics, including disinformation campaigns, destructive and disruptive malware, state-affiliated hacktivism, and financial warfare, to weaken trust in systems and sow chaos globally. These tactics are designed to set the stage for future attacks, creating vulnerabilities rather than causing immediate, high-impact damage.
- **Ransomware** – Criminals are shifting from data encryption to data-leak extortion, with ransomware emerging as one of the most significant cyber threats to businesses worldwide in 2024. Law enforcement operations had a significant impact on RaaS actors, leading to a more fragmented ecosystem, shift towards data-leak extortion and increased targeting of healthcare service-providers.
- **Infostealers** – These malware attacks have surged by 58%, stealing credentials and sensitive data, impacting both individuals and organizations. The increase is driven by a rise in infostealer infections, particularly targeting tokens and VPN credentials from BYOD environments. With the decline of botnets and banking malware, infostealers have become the primary facilitators of initial access brokers, extracting corporate access credentials and tokens.
- **Edge Devices Vulnerabilities** - Both state-sponsored and financially motivated attackers have increasingly targeted edge devices as a primary access vector to enterprise networks. These compromised devices are often used to create Operational Relay Boxes (ORBs), which anonymize and relay communications, supporting covert activities and further exploitation of network vulnerabilities.
- **Cloud** - Misconfigurations and poor API security are leaving cloud environments exposed, with cloud administration complexity and hybrid environments enabling attackers to move between on-premises and cloud systems. Dependence on external SSO security and the hijacking of cloud-hosted LLM models further heighten vulnerabilities.

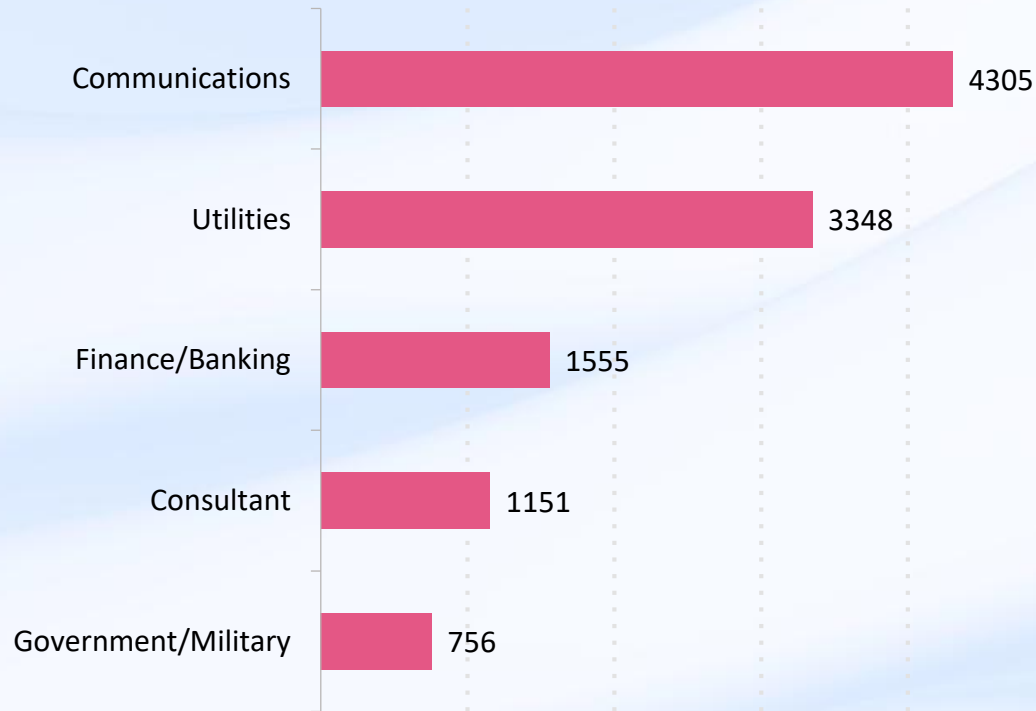
Attacks per Organisation – last 6 months

- Recent work conducted by Thinking on a 20 seat organisation saw the info inbox being brute force attacked 4 times a second continually

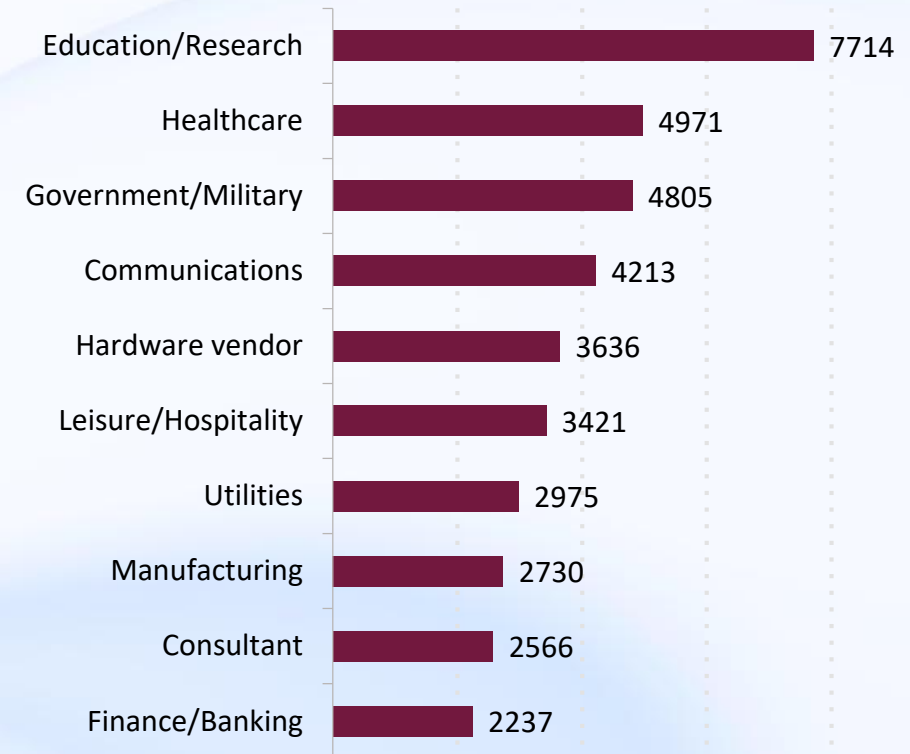


Most Impacted Industries - Last 6 Months

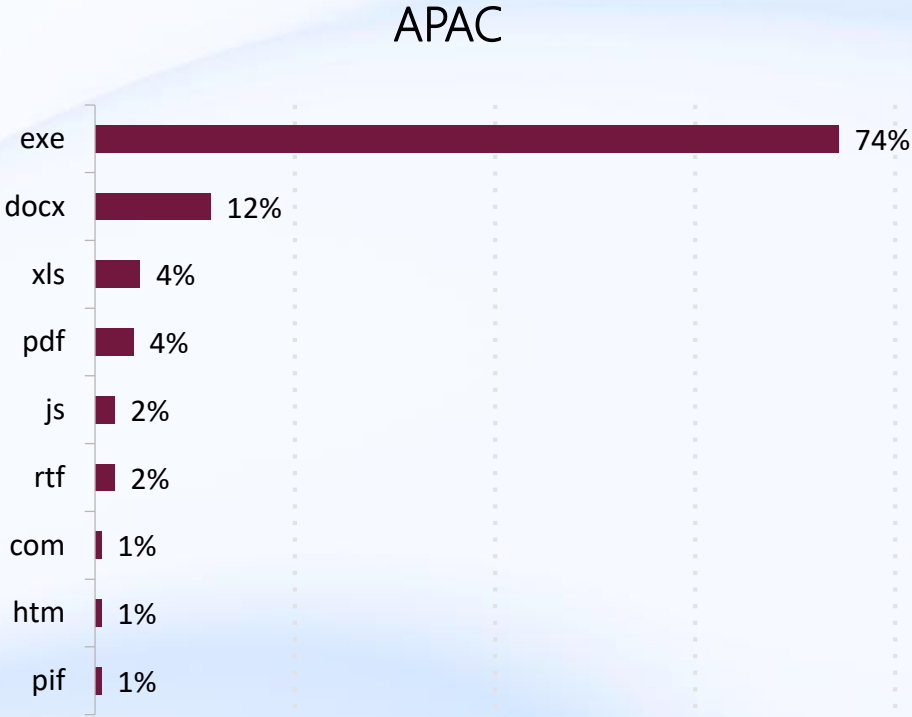
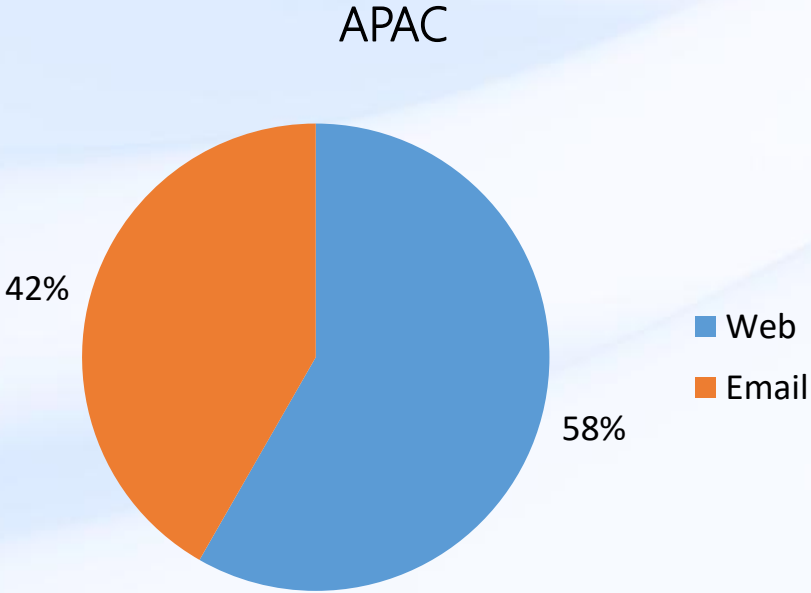
Weekly Attacks per Organization - New Zealand



Weekly Attacks per Organization - APAC



Attack Vectors for Malicious Files - Last 30 Days



Protecting Email

Why bother?

- Objections
 - We are small no one will care about us
 - It's too expensive
 - Too much effort, I don't have time
 - We have antivirus
- Reality
 - Email is critical to business function
 - Cost of being without

Where is your Email

- ISP based email is very hard to protect
 - POP/IMAP/SMTP accounts
- On premise email is expensive to maintain
- For SMB use a larger cloud provider
 - Microsoft/Google/Zoho
 - Commercial security tools available for Microsoft and Google
 - All named providers have native antivirus support – better than nothing
 - Products are well supported, reliable and understood
 - Migration tools are available
- DNS is critical to Email
 - Ensure you own your domain and have admin access to the zone

How to find out...

- <https://mxtoolbox.com/>
 - Demo

Legitimate Email

- Did I expect to receive it, but we are busy aren't we
- Attacks are sophisticated – it needs a machine to deal with it

Spot the Difference?

maybank2u.com is not the same as maybank2u.com


citibank.com is not the same as citibank.com
(the first one is correct, the second one is from hackers)

The "a" in the later url is a cyrillic alphabet.

An average internet user can easily fail for this. Be careful for every mail requiring you to click on a link.

Please Stay Alert

Quarantined [Good day]

 noreply@northwestcountry.co.nz
To: Danielle Hancock Expires: 6/03/2025 Tue 4/02/2025 3:21 am

Retention Policy: Junk Email (30 days)
This item will expire in 29 days. To keep this item longer apply a different Retention Policy.
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the inbox.
We converted this message into plain text format.

Hello Danielle Hancock

An email has just been received from Linnea Hedlund <linneahedlund24@outlook.com> and is suspected to be a "Phishing" email. The email message is safely quarantined.

The email subject is: Good day
Email attached files are:
Detection reasons are:

- * Sender does not have established reputation
- * Email body language indicates potential phishing attempt
- * Email is marked as spam by O365

If you wish to request to release it from quarantine, click here <https://northwestcountrybusinessassociation.checkpointcloudsec.com/email_restore.html?msg=77b958cf4137042bcac4b17684493f93%40northwestcountrybusinessassociation&type=office365_emails&mode=phish_request_restore> or contact your system administrator.
You may be required to authenticate, in that case follow these instructions:
1. You will be directed to a page where you would be requested to specify your email address.
2. An email with verification code will be sent to you.
3. Copy the code and return to the email recovery page.
4. The email will be released to your mailbox.

Please exercise discretion when requesting to release suspicious emails.

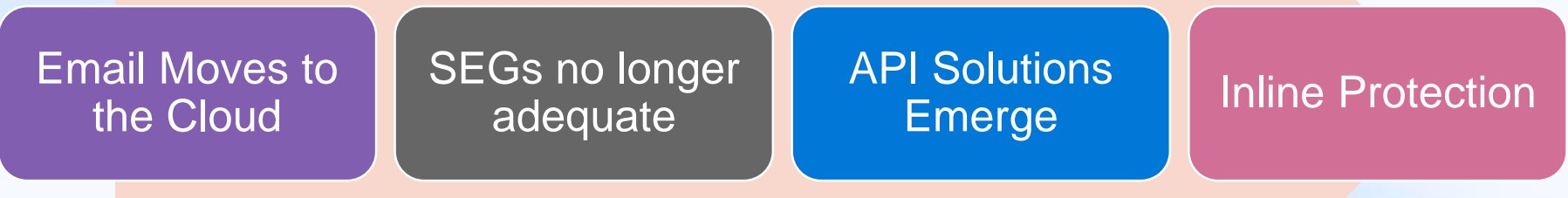
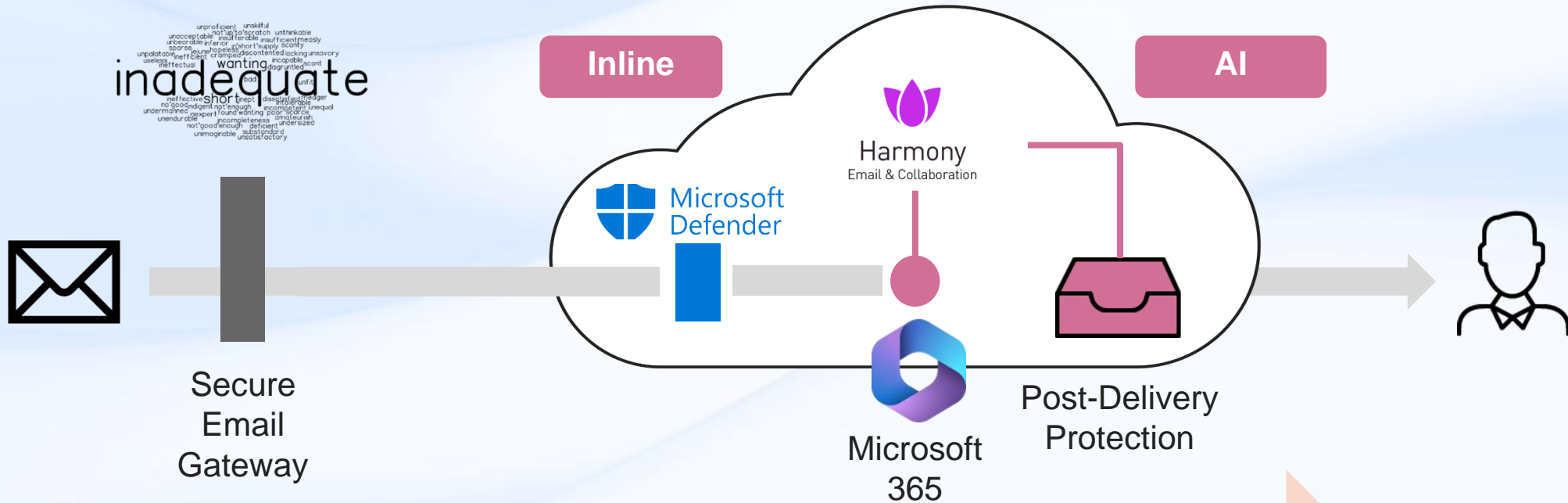
You can read more about phishing attacks here <<https://en.wikipedia.org/wiki/Phishing>>.

Securing Cloud Email

Protecting Yourself

- Major providers have built in protection
 - Usually it isn't very good and requires administration
- Add third party products to compensate
 - Avoid MX driven solutions or on premise gateways
 - API driven – integrates directly with the cloud provider
 - You end up with 2 solutions, native cloud and third party
 - AI enabled – it learns about your mail and acts on your behalf
 - Malicious Email is stopped before it enters your inbox
 - Examples Checkpoint Harmony, Proofpoint, Mimecast

The Evolution of Email Security

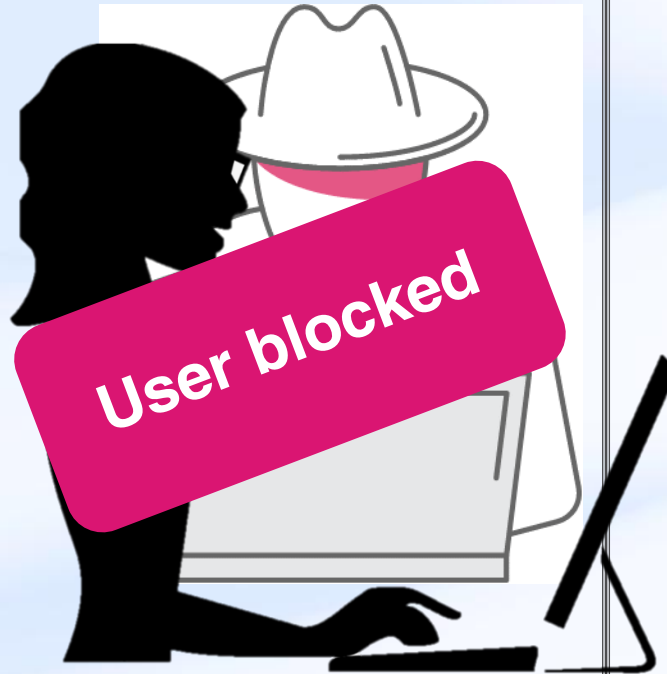


Protecting Against Compromised Accounts

Practical Steps to Reduce Exposure

- General
 - NZISM Section 16 <https://nzism.gcsb.govt.nz/>
 - Strong password
 - Unique accounts for users
 - Enable MFA – no argument
 - Yubikeys for password less access
 - Logging (3 months retained by standard cloud accounts)
 - Cyber Security Training and testing for staff
- Policies
 - Remove legacy protocols
 - Set up country based access
 - Restrict guest access
 - Restrict by device type
- Microsoft
 - Add Azure P1 licenses to allow for conditional access policies
- Google
 - Enterprise Standard Subscription for context aware policies

Auto Blocking



User Actions

- | | |
|--|-----------------------------------|
| Login from the office (business hours) | Login during unconventional hours |
| Login from home (off-hours) | High-rate email sending |
| Sending emails (business hours) | Suspicious mailbox rules |
| Login from abroad (business trip) | Impossible travel |
| Occasional password-resets | Multiple password-resets |
| Login from new country (company-wide) | First-time browser / device / VPN |

Verdict:
Compromised



Behavior baseline (per-user)

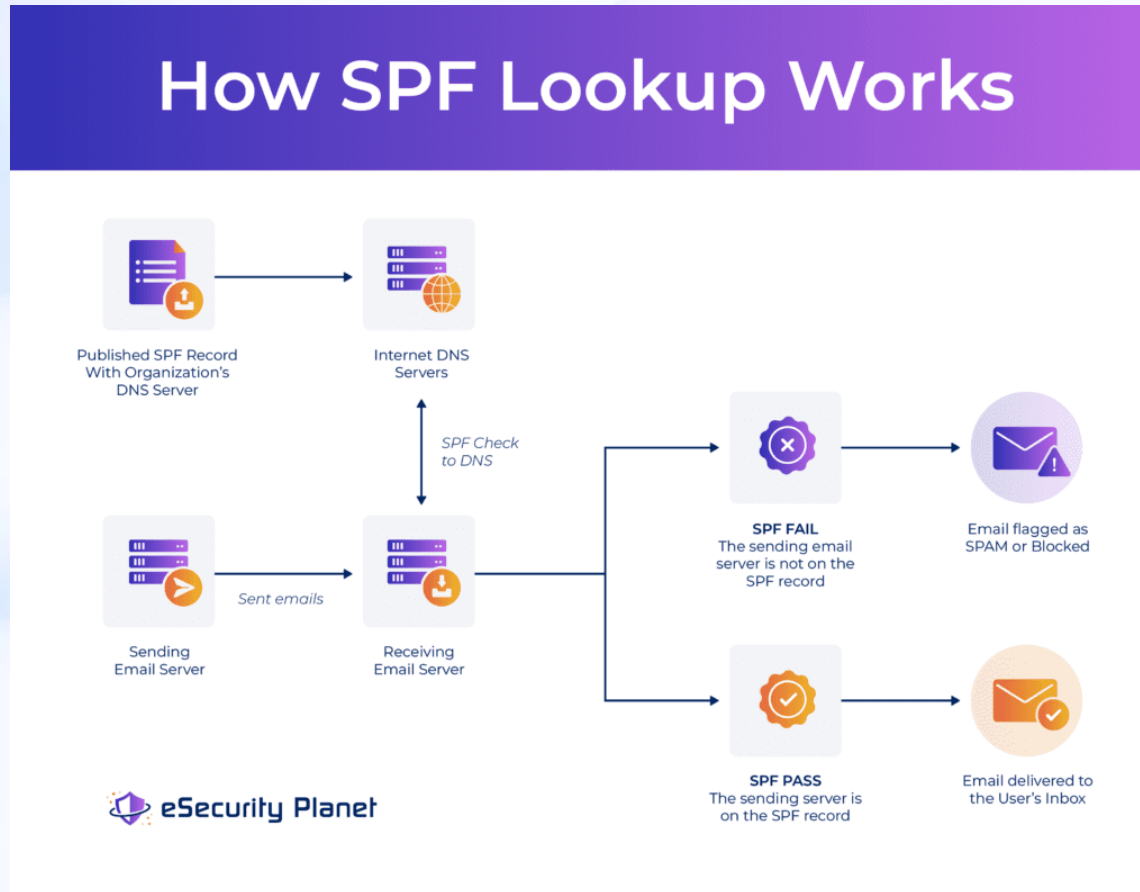
Possible Suspicious Activity

DMARC

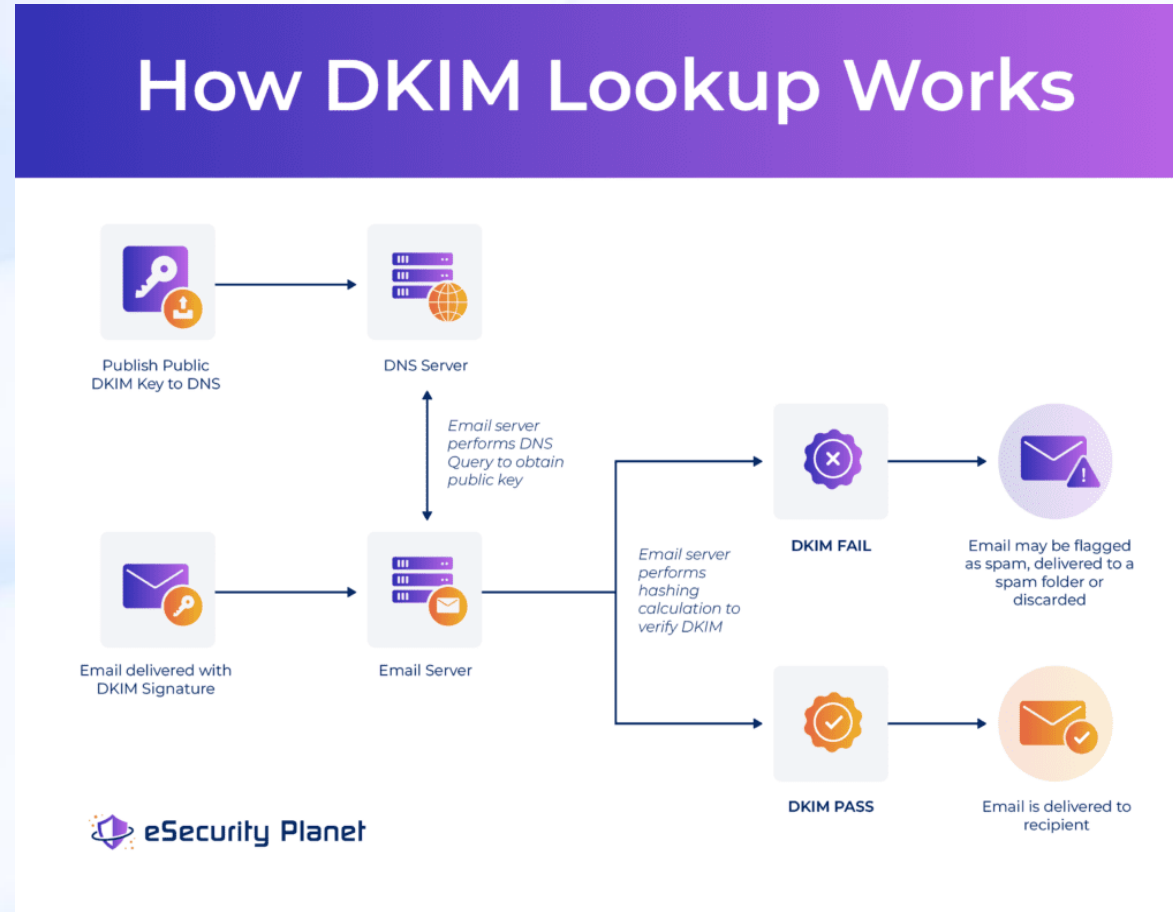
Notes

- Its not a product
- It's a configurable standard that prevent email impersonation
- It should be monitored
- Requires access to DNS

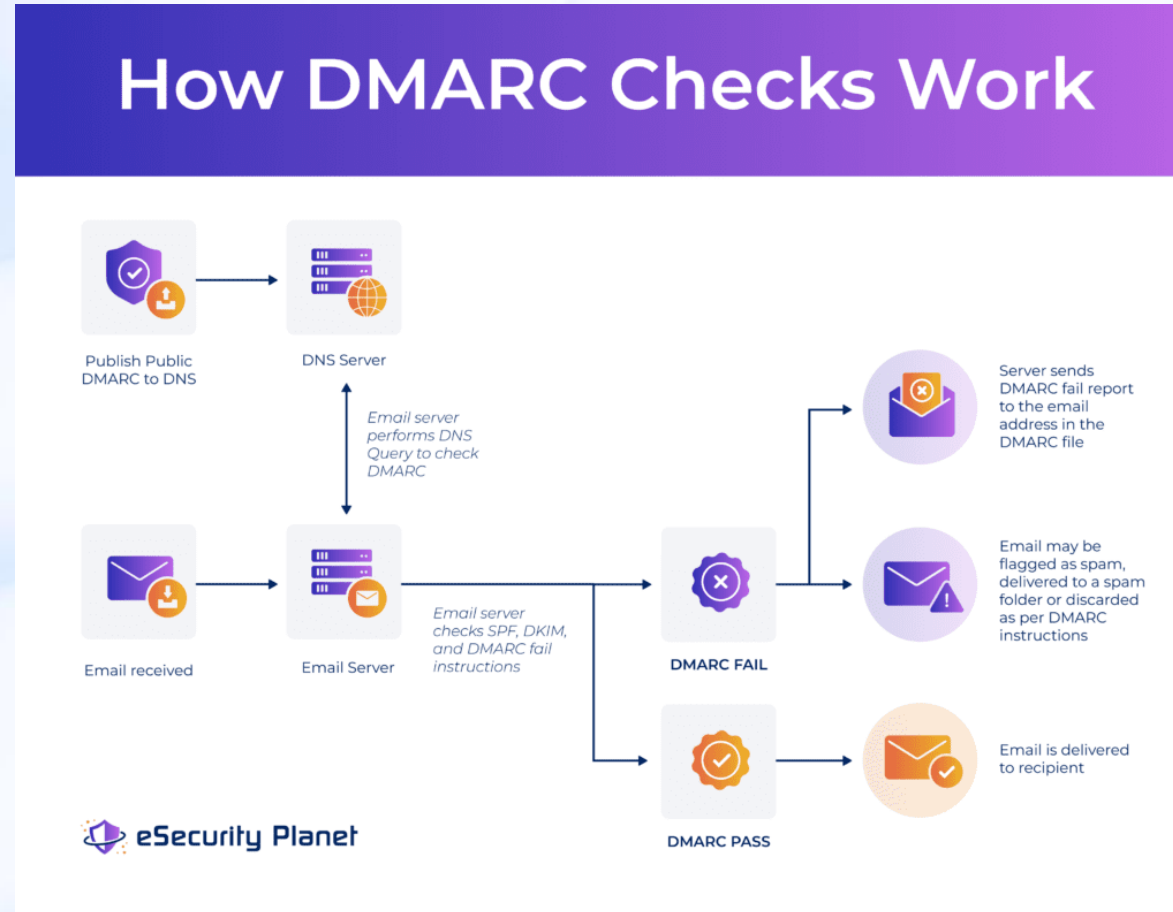
SPF - <https://mxtoolbox.com/spf.aspx>



DKIM - <https://mxtoolbox.com/dkim.aspx>



DMARC - <https://mxtoolbox.com/dmarc.aspx>



Blacklisting and Breaches

What's my situation

- Good old mxtoolbox to the rescue
 - <https://mxtoolbox.com/blacklists.aspx>
- Have I been pwned
 - <https://haveibeenpwned.com/>
- Knowbe4
 - <https://www.knowbe4.com/free-cybersecurity-tools/email-exposure-check>

What to do if I am breached

- Before
 - Cyber Insurance
 - Policies
 - Be aware of your responsibilities as a company director
 - Immutable backups
 - Budget for Cyber protection
 - Train staff
 - Cert NZ Top Ten
 - <https://www.cert.govt.nz/information-and-advice/critical-controls/10-critical-controls/>

What to do if I am breached

- During
 - Preserve data and act
 - Alert Office of the Privacy Commissioner if private data is involved
 - Alert your insurer and advisors
 - Communicate (carefully)
- After
 - Review controls and adjust to suit

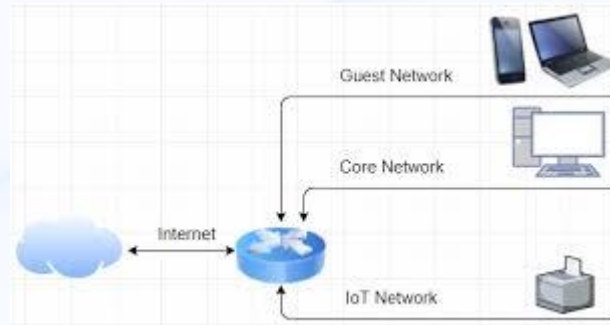
Email from Devices and Software

Risks

- Older devices require the use of legacy protocols
 - Try to avoid or use conditional access policies to restrict
 - Avoid using an old Gmail account
- Procure devices and/or software that integrates with major IDP's
 - IDP = Identity Provider e.g. Entra and Google Identity
- Conditional Access Policy to disable MFA for these devices
- Outbound firewall rules to restrict traffic to set locations

Printers..

- Put printers in VLAN's
 - Topic in its own right – zero trust



Visibility

Demos

- Look and see
 - DMARC Portal
 - HEC Portal

Final Thoughts

Notes from the field

- Breaches are notifiable especially where private data is involved
 - Office of the Privacy Commissioner investigates
 - They attract fines where negligence is identified
 - Public disclosure can significantly impact a brand
 - Don't hesitate if a breach is detected, inform the Privacy Commissioner and your Insurer
 - Develop a breach policy and procedures
- Cyber Insurance is worth considering
- Cyber threats are monetised
- Protect your Email – it's the #1 attack vector

Discussion