VOLKIS™

Security Review & Phishing Campaign

Prepared for Company Name, 2 January 2023

Table of Contents

Executive summary

Company Name engaged Volkis to a perform penetration testing on their internet-facing web application, perform a security review of Company Name's Microsoft 365 tenancy and simulate a phishing campaign. This test was performed on a best effort basis, which aims to perform as much testing as possible within the scoped timeframe.

Volkis used the same hacking tools that hackers will use to investigate and understand the scope, then find and exploit identified security vulnerabilities. The testing investigated security vulnerabilities that could present risk to Company Name by allowing an attacker access to sensitive information such as client data, to manipulate application processes, or to affect the operations of Company Name.

Volkis ran a phishing simulation against 60 Company Name staff. The consultant crafted an email that simulated communication from a staff member about a new partnership to facilitate a laptop replacement program. The user was encouraged to click the link and enter Microsoft 365 credentials to register for the program. The email was deliberately targeted at Company Name users rather than using a generic phishing attempt, such as an unpaid invoice, to test the user's ability to spot attacks against the business.

20% of users clicked the provided link and approximately 8 users attempted to enter credentials. These numbers are higher than average and indicate a lack of awareness and training on how to spot and handle phishing emails. Providing Information Security Awareness Training (ISAT) to users will help them to better protect themselves personally and the business by encouraging secure habits.

Company Name's Microsoft 365 tenancy was reviewed for security misconfigurations that a malicious actor may be able to abuse. It is clear efforts have been made to harden the tenancy against attacks however there is room for improvement in most areas such as email protections (DKIM/DMARC) and restrictions on email forwarding.

Company Name's public presence is limited which makes it difficult for attackers to obtain information. Few private email addresses and no sensitive information could be found using common tools. While some necessary ports are exposed to the internet, external services were either protected by Cloudflare or non responsive. Breached password databases did not contain any cleartext passwords, and the password hashes that were available (from Canva.com breach from 2019) were not able to be cracked within the testing timeframe. Overall Company Name's external footprint is well managed.

The Company Name's website implements common WordPress attack mitigations and is resilient to attack. During the time-frame of the assessment some out-of-date plugins were found, but no vulnerabilities were identified.

In order to improve the security posture of Company Name, Volkis recommends:

- Performing a phishing simulation debrief with users and implementing Information Security Awareness Training.
- Additional hardening of the Microsoft 365 tenancy in line with recommendations provided.
- Implementing a patch management policy for Wordpress website.

For more information about this report, the identified vulnerabilities, and additional services that could help you in your security journey, please contact your Volkis consultant:

Contributor #1

- Email: Email #1
- Mobile: Ph #1

Overview

Company Name engaged Volkis to perform a security review on their Internet accessible web applications, and Microsoft 365 tenancy as well as perform a phishing campaign.

Testing was performed over a 5-day window on a best effort basis. Best effort testing aims to perform as much testing as possible within the scoped timeframe.

Scope

The scope of the test included:

- A phishing simulation against 60 users
- A security review of of the primary Microsoft 365 tenancy
- Web application penetration test of **www.company.com.au**
- Public presence review

Root cause analysis

This section highlights what we determined to be the likely root cause of the vulnerabilities discovered. By addressing the root cause, you reduce the chances of introducing new vulnerabilities of the same class.

Information security awareness training

Even though most employees have no experience in information security, security is never-the-less becoming a key part of the work of every person who works with computers. This means the employees need training on the information security requirements and expectations for their work.

Effective Information Security Awareness Training (ISAT) programmes incorporate a mixture of classroom style presentations or computer-based training, regular updates using emails or announcements in team meetings, and posters in visible locations.

Company Name should consider implementing an ISAT programme for its staff. This will help to grow the security culture of the organisation and protect the company from social engineering attacks.

Effective security practices

Volkis likes to celebrate the positives! This section highlights some of the effective security practices and controls that were observed during the penetration test.

Limited attack surface

Company Name's external infrastructure was found to be well-secured, with a limited number of services exposed to the internet and using mostly secure configurations. This prevented any successful attacks against the Company Name infrastructure.

Additional recommendations

Defence-in-depth is a security concept that teaches multiple layers of protection against adversaries. These recommendations are not specifically related to a vulnerability but will increase the overall security of the organisation.

Outdated WordPress plugins

The **companyname.com.au** website is using an outdated version of the woocommerce and gravity-forms plugins. Although there are no security flaws present in the older version of these plugins, they should still be updated as a best-practice. Additionally, Company Name should review their policy to ensure more regular updates of plugins in the future.

Unnecessary ports exposed

Limiting the attack surface of a system can help protect it from exploitation by cutting off avenues for access. As such, it is best practice to reduce the number of ports and services exposed on a host.

The following hosts were affected:

- events.company.com.au

- resources.company.com.au
- donate.company.com.au

All three hostnames are exposing TCP ports `80`, `443`, `8080`, `8443`. The services are protected by Cloudflare but each of these ports/services should be reviewed to ensure it is necessary they they are exposed. If not, disable the service and firewall off the ports.

Conclusion

Volkis performed a security review, phishing simulation, and web application penetration test on Company Name and discovered areas in which the organisation may improve their security posture. By working through the recommendations in the report and addressing their root causes Company Name can make incremental improvements to protect the business and it's staff.

We're here to help! If you find yourself needing assistance with fixing a vulnerability in this report or are unsure what the next step in your security strategy should be, reach out. Volkis's consultants are experts in the information security field who love to talk shop.

Thank you for letting us hack you and thank you for reading.

Contributor #1

- Email: Email #1

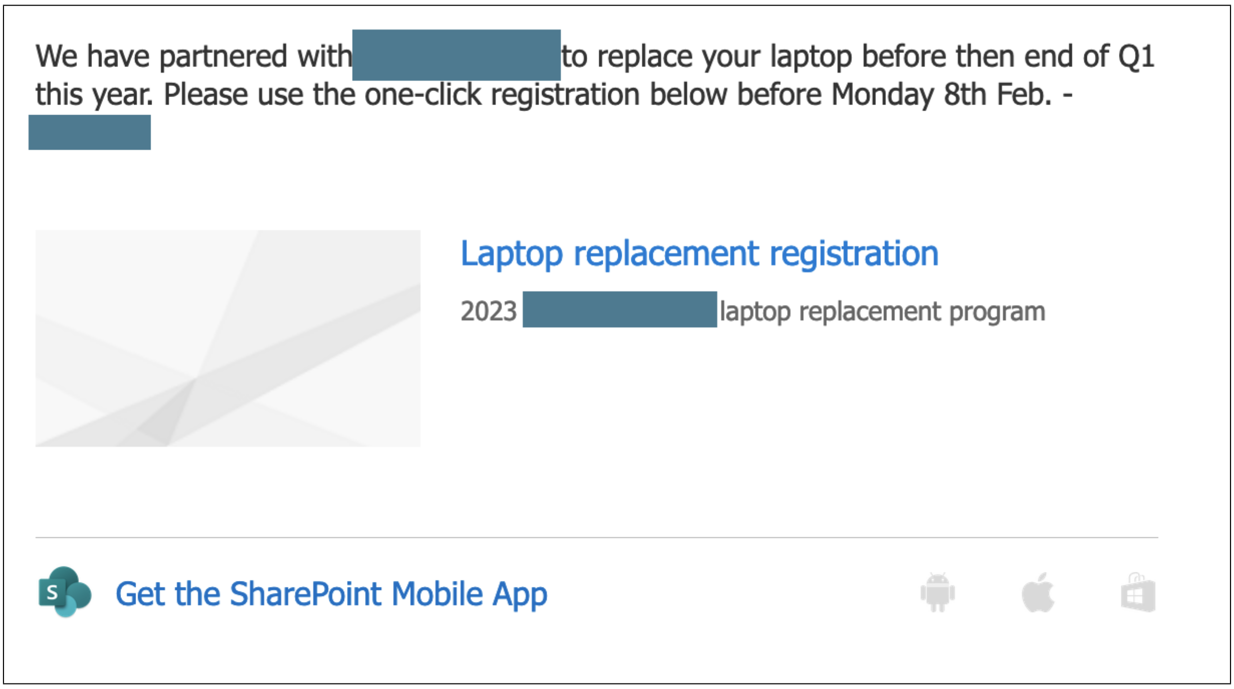
Phishing Campaign

Scenario

Volkis performed a phishing campaign on Company Name staff as part of their security awareness program. The scenario was based on current trends observed in the wild with the likely staff demographic in mind. The staff's responsiveness to a perceived phishing attack was also tested.

Scenario details

Target employees were sent an email that appeared to be a Microsoft SharePoint link sent by a staff member via a new partner. The email suggested a laptop replacement program was being put in place and requesting staff click a link to register. To build trust, the email tried to appear just as an standard Microsoft file sharing email would.



We have partnered with [redacted] to replace your laptop before then end of Q1 this year. Please use the one-click registration below before Monday 8th Feb. - [redacted]

Laptop replacement registration

2023 [redacted] laptop replacement program

Get the SharePoint Mobile App

Figure 1: Phishing email sample

The sender email mimicked a fake partner's domain name and SharePoint tenancy by using **company-sharepoint.ourphishingdomain.com**. This domain was registered specifically for the campaign and used to send email.

The link sent users to a web server controlled by the consultant. The intended behaviour was for the web server to act as a credential harvesting tool. Users would then be redirected to the legitimate version of the page, so as not to arouse suspicion.

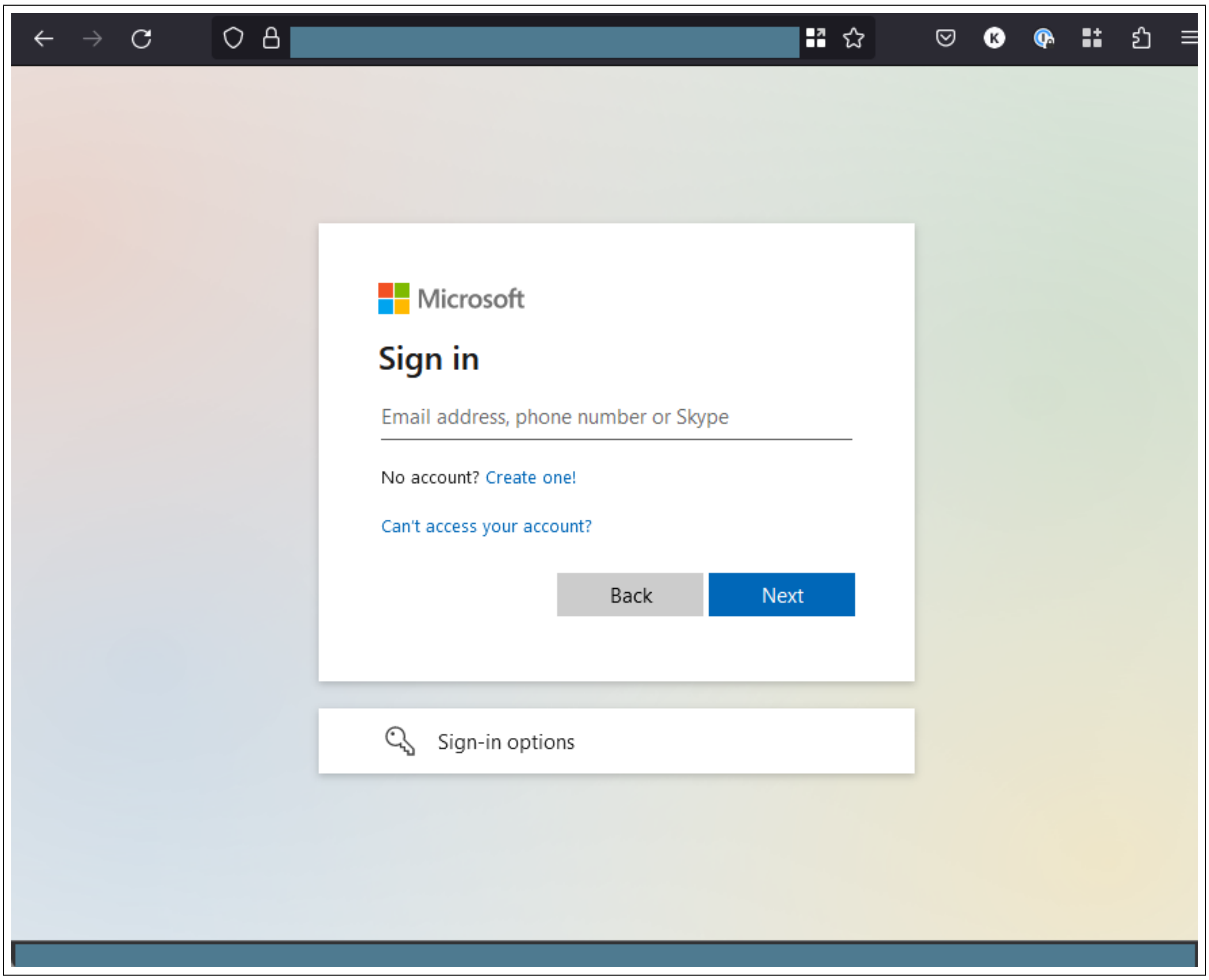


Figure 2: Phishing campaign landing page

Choosing a recognised login page has its trade-offs. On one hand, users are more likely to believe that the email and landing page are legitimate. On the other, it is more likely to be detected by Google's Safe Browsing initiative and be blocked on all browsers.

Results

Description

The phishing campaign was started at 11:30AM (AEST) on the 2nd of February 2023 and emails were sent to Company Name staff over a period of 10 minutes.

The campaign stayed active until approximately 5:30PM 2nd February 2023, when new results stopped showing and the campaign had already been successful.

The following final results were observed:

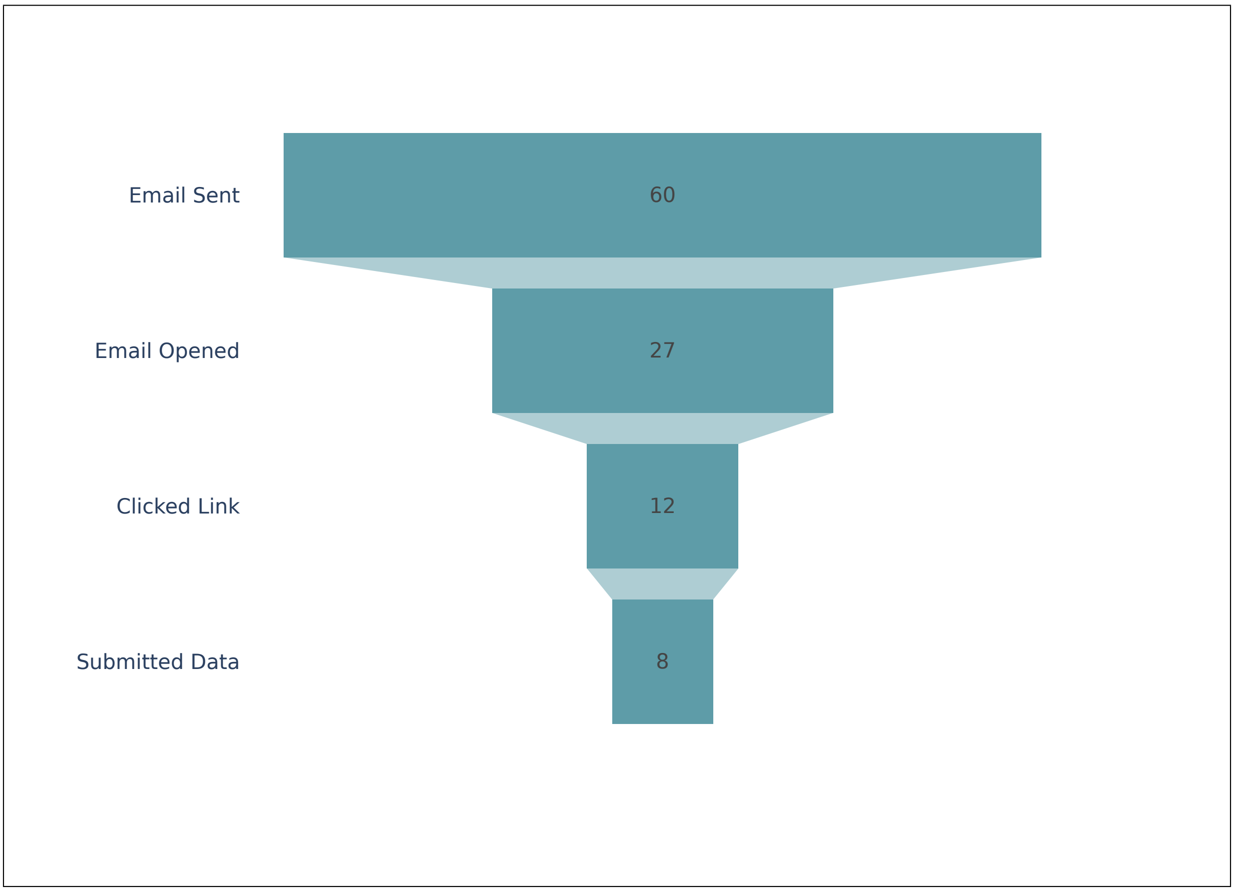
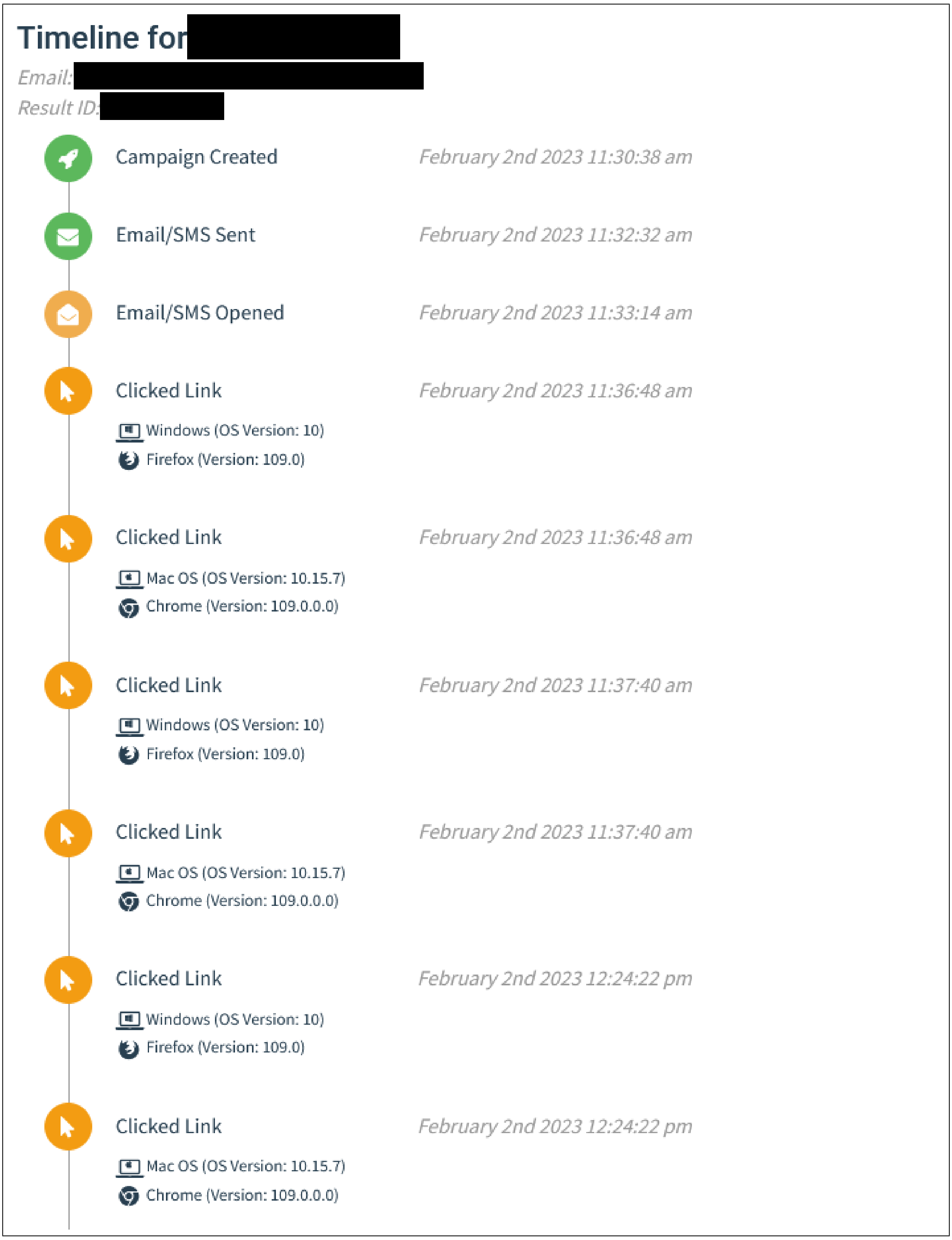


Figure 3: Phishing campaign results

Note that the **Emailed Opened** number is an estimate only. It relies on an embedded image being opened by the email client. If the email client is configured to not retrieve embedded images, there is no way to know if the person opened the email but did not click on the link. For a full list of which employees reached which stage, refer to **Appendix A: Phishing campaign results**.

Additionally, during testing some technical issues with the web server occurred. While the landing page did present as required, users were presented an error when attempting to enter credentials instead of being redirected; and no credentials were captured. However, it was possible to correlate the user's external IP addresses with their campaign IDs and as such an estimate of how many users attempted to enter their credentials could be made and who they may have been.

This technical issue did result in an interesting finding as many users attempted to enter their credentials multiple times across multiple devices which in itself shows that the users did not identify the email as malicious even after a failed login attempt.



Timeline for [redacted]

Email: [redacted]

Result ID: [redacted]

Campaign Created — *February 2nd 2023 11:30:38 am*

Email/SMS Sent — *February 2nd 2023 11:32:32 am*

Email/SMS Opened — *February 2nd 2023 11:33:14 am*

Clicked Link — *February 2nd 2023 11:36:48 am*
Windows (OS Version: 10)
Firefox (Version: 109.0)

Clicked Link — *February 2nd 2023 11:36:48 am*
Mac OS (OS Version: 10.15.7)
Chrome (Version: 109.0.0.0)

Clicked Link — *February 2nd 2023 11:37:40 am*
Windows (OS Version: 10)
Firefox (Version: 109.0)

Clicked Link — *February 2nd 2023 11:37:40 am*
Mac OS (OS Version: 10.15.7)
Chrome (Version: 109.0.0.0)

Clicked Link — *February 2nd 2023 12:24:22 pm*
Windows (OS Version: 10)
Firefox (Version: 109.0)

Clicked Link — *February 2nd 2023 12:24:22 pm*
Mac OS (OS Version: 10.15.7)
Chrome (Version: 109.0.0.0)

Figure 4: Multiple login attempts from a single user

The results show that it is possible to compromise a significant number of accounts. The 13% success rate is higher than average and indicates that staff may need additional training.

In a real-world scenario, if malicious attackers were to gain employee credentials they would likely have access to email, SharePoint and other connected services, compromising sensitive data.

Recommendations

The most important thing after a phishing campaign is to treat the exercise in a very positive light. Employees who divulged their credentials should not be singled out, but rather encouraged to continue trying to notice phishing emails. We also recommend performing a whole-company debrief session to explain the scenario and share the results.

Employees who came forward and called out the phishing emails to IT staff should be commended and others encouraged to do the same. This helps to build a positive security culture in the organisation.

Continue performing Information Security Awareness Training (ISAT) to maintain and increase security awareness of employees in the organisation. As part of ISAT, more phishing campaigns should be performed so that employees can practice and get used to identifying them.

Microsoft 365 Review

Volkis performed a security review on Company Name’s Microsoft 365 environment with the goal of identifying areas where security could be improved. The findings in this section are not vulnerabilities; rather, they are opportunities to improve overall security by making a successful attack more difficult for adversaries.

The list of checks that were performed are base on industry recognised hardening guides from Microsoft, Center for Internet Security (CIS) and our own experience hacking Microsoft 365 environments. They are also tailored to the Company Name’s existing tenancy and licenses.

Summary

The following table shows the checks that were performed during the security review and the results:

Check	Securely Set	Priority
Multi-factor Authentication enabled for all users	No	High
Multi-factor Authentication enforced for Global Admins	No	High
Legacy Authentication is disabled	Yes	High
There are between 2 and 4 Global Admin accounts	Yes	High
Separate accounts for Admin access	Yes	High
Enforce Password Protection	No	High
Passwords are not set to expire	Yes	High
Users not allowed to give app consent	Yes	High
Attachment Type filter enabled	Yes	High

Continued on next page

Check	Securely Set	Priority
External mail forwarding restricted	No	High
Anti-phishing policy exists	Yes	High
DKIM enabled for all domains	No	High
SPF Records are published	Yes	High
Email bounce message is nondescript	No	High
Audit log search enabled	Yes	Low
onmicrosoft email aliases removed	No	Low
Public groups are intentional	Yes	Low
Calendars are not shared externally	No	Low
Office add-ins restricted	No	Low
DMARC Records are published	No	Low
Outbound malicious email alerting	Yes	Low

Multi-factor Authentication enabled for all users

Purpose

Having multi-factor authentication (MFA) enabled for all users will require them to use at least 2 factors for authentication. That is 2 out of 3 of the following factors:

- Something you know;
- Something you have;
- Something you are.

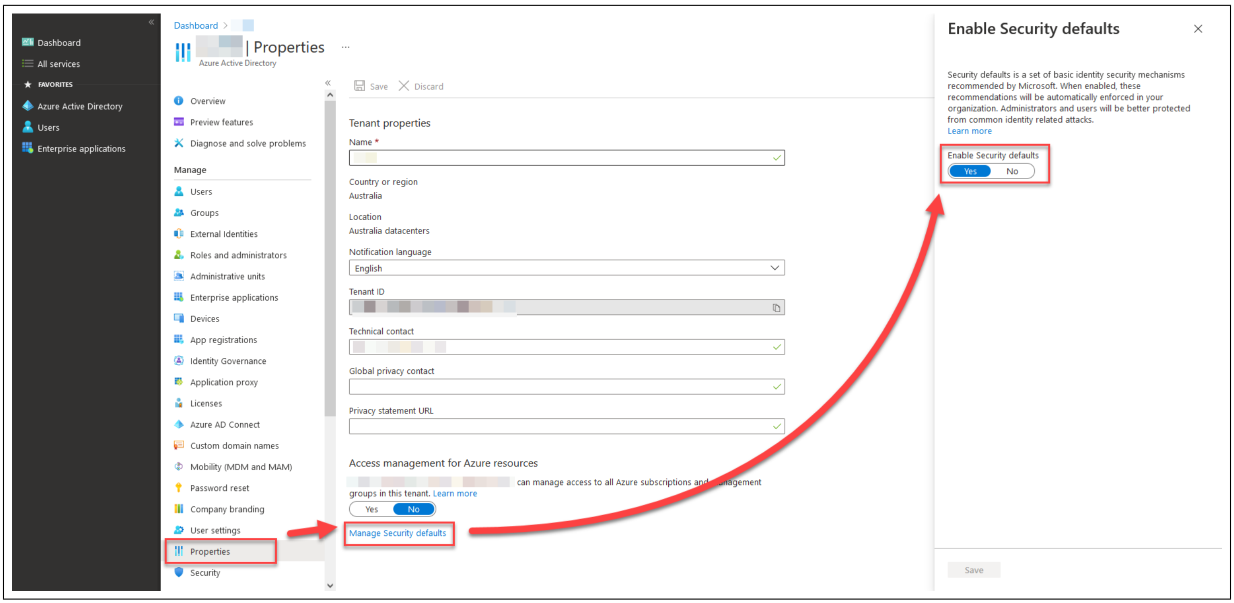
Generally, for Microsoft 365 environments, a password and a one-time token is used to prove the 2 factors. This means, if an attacker compromises one factor, such as someone's password, they would still require the 2nd factor to be able to authenticate to the victim's account. The 2nd factor provides an added layer of protection.

Recommendation

For Microsoft 365 Business Standard tenancies, it is recommended to set MFA by enabling Secure Defaults.

Login to Microsoft 365 Admin Center, then:

1. Select **Azure Active Directory**
2. Select **Azure Active Directory** again
3. Select **Properties** then select **Manage security defaults**
4. Set **Enable Security Defaults** to **Yes**



Tenant properties

Name * [redacted]

Country or region
Australia

Location
Australia datacenters

Notification language
English

Tenant ID
[redacted]

Technical contact
[redacted]

Global privacy contact

Privacy statement URL

Access management for Azure resources

[redacted] can manage access to all Azure subscriptions and management groups in this tenant. Learn more

Yes [✓ No]

Manage Security defaults

Enable Security defaults

Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.
Learn more

Enable Security defaults
[✓ Yes] No

Figure 5: Enabling Security Defaults

Multi-factor Authentication enforced for Global Admins

Purpose

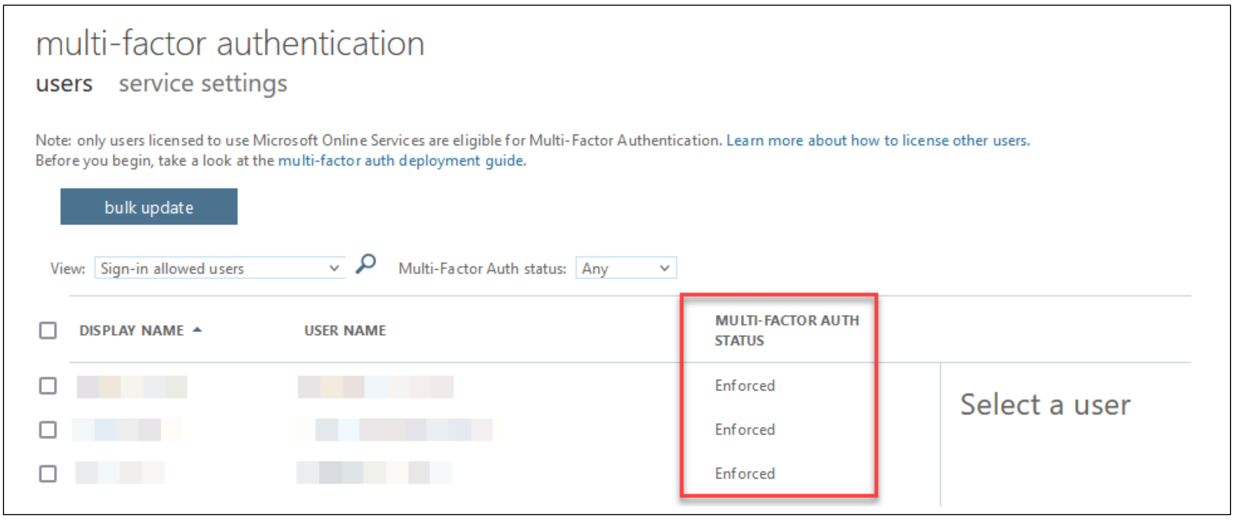
Although enabling MFA for accounts logins protects them from access from an unknown location, Microsoft may not require a user to enter their 2nd factor if the connection originates from a known location. An example of this scenario is when an attack compromises a victim’s machines and performs login requests through their internet connection.

Recommendation

Enforce MFA for all Global Admins so that a 2nd factor is required each time the user logs in.

Login to Microsoft 365 Admin Center, then:

1. Select **Users** then **Active Users**
2. Select **Multi-factor Authentication**
3. For each Global Admin, select the account, then select **Enable** and then **Enforce**
4. Ensure that *Multi-factor Auth Status* shows as *Enforced*



multi-factor authentication

users   service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

View: Sign-in allowed users   Multi-Factor Auth status: Any

□	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
□	[redacted]	[redacted]	Enforced
□	[redacted]	[redacted]	Enforced
□	[redacted]	[redacted]	Enforced

Select a user

Figure 6: MFA set to enforced

Enforce Password Protection

Note that this feature is only available with the Enterprise Mobility and Security E3 licenses.

Purpose

Microsoft 365 will prevent users from choosing passwords that are weak or that are known to be in common password lists that attackers may try to use in a brute-force attack. This will encourage users to choose stronger passwords.

Recommendation

Login to Microsoft 365 Admin Center, then:

1. Select **Azure Active Directory**
2. Select **Azure Active Directory** again
3. Select **Security** then select **Authentication methods**
4. Ensure that **Enable password protection on Windows Server Active Directory** is set to **Yes**
5. Set **Mode** to **Enforced**.

External mail forwarding restricted

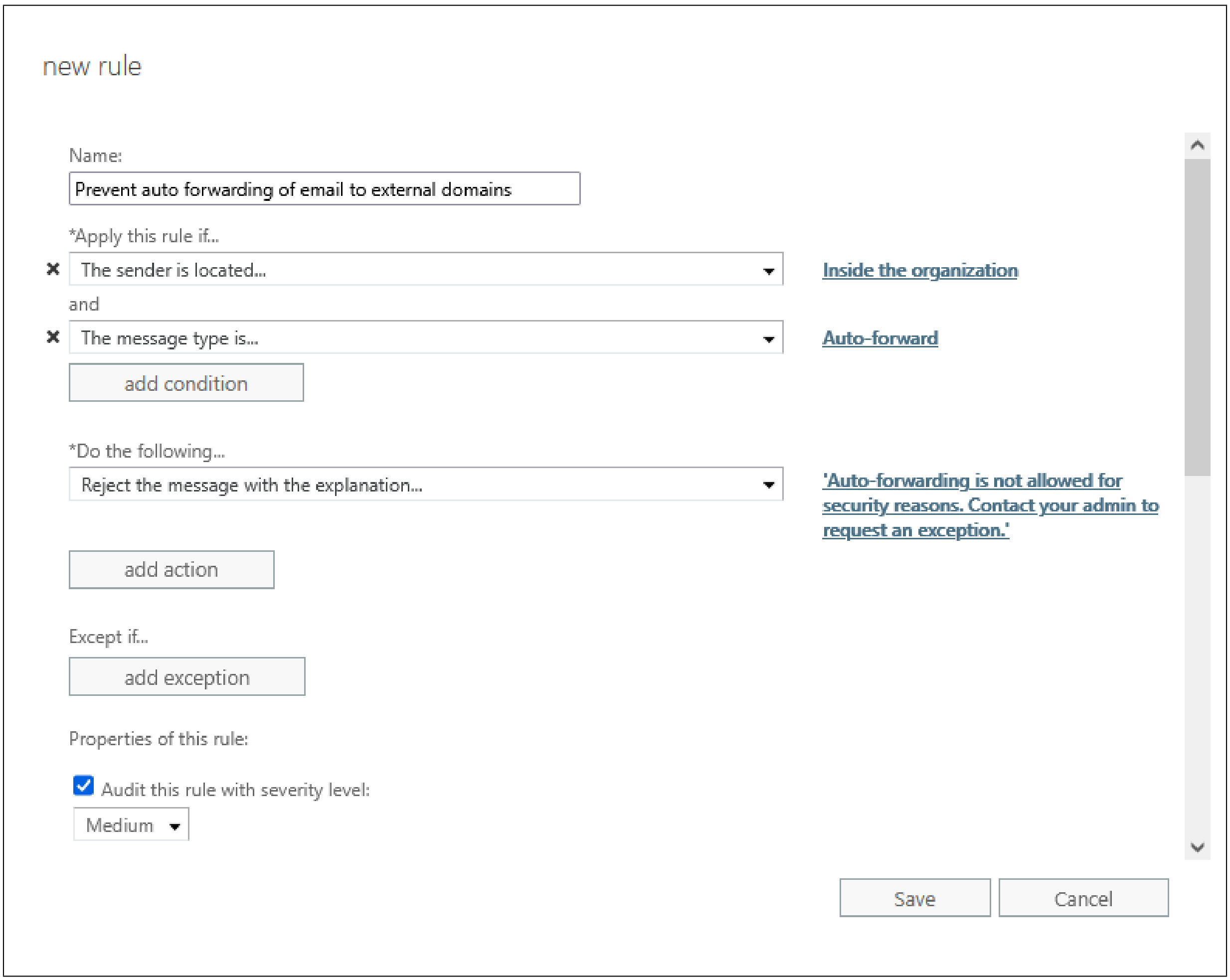
Purpose

After an account is compromise, an attacker will commonly setup an email forwarding rule to the attacker's external mailbox. This is done to compromise sensitive information sent to the victim account and to gain a better understanding for how the target company operates. By disabling forwarding rules to external addresses, Company Name can protect themselves in case of a compromise.

Recommendation

Login to Microsoft 365 Admin Center, then:

1. Select **Exchange**
2. Expand **Mail flow**, then select **Rules**
3. Select the **+** button, then select **Create a new rule...**
4. Scroll down and select **More options...**
5. Enter a descriptive name in the **Name** field
6. Under **Apply this rule if...**, select **The sender** > then **is external/internal**
7. Choose **Inside the organization** and select **OK**
8. Select **add condition** to add a new dropdown menu
9. From the new dropdown, select **The message properties...** > then **include the message type**
10. Choose **Auto-forward** and select **OK**
11. Under **Do the following...**, select **Block the message...** > then **reject the message and include an explanation**
12. Enter a message that would be informative for a user attempting to setup an Auto-forward rule, then select **OK**
13. Optionally, add exceptions
14. Under **Audit this rule with severity level**, select an appropriate rating for your company
15. When finished, select **Save**



new rule

Name:

Prevent auto forwarding of email to external domains

*Apply this rule if...

✖ The sender is located... ▾ Inside the organization

and

✖ The message type is... ▾ Auto-forward

*Do the following...

Reject the message with the explanation... ▾ 'Auto-forwarding is not allowed for security reasons. Contact your admin to request an exception.'

Except if...

Properties of this rule:

☑ Audit this rule with severity level:

Medium ▾

Figure 7: Creating a rule to block auto-forward

DKIM enabled for all domains

Purpose

DomainKeys Identified Mail (DKIM) is a protection against email spoofing, spam and phishing. Without DKIM, it may be possible for attackers to impersonate user emails originating from the company.com.au domain in a phishing attack against Company Name clients.

Recommendation

Each domain that is configured to send or receive email in the Microsoft 365 tenancy should have DKIM signing enabled.

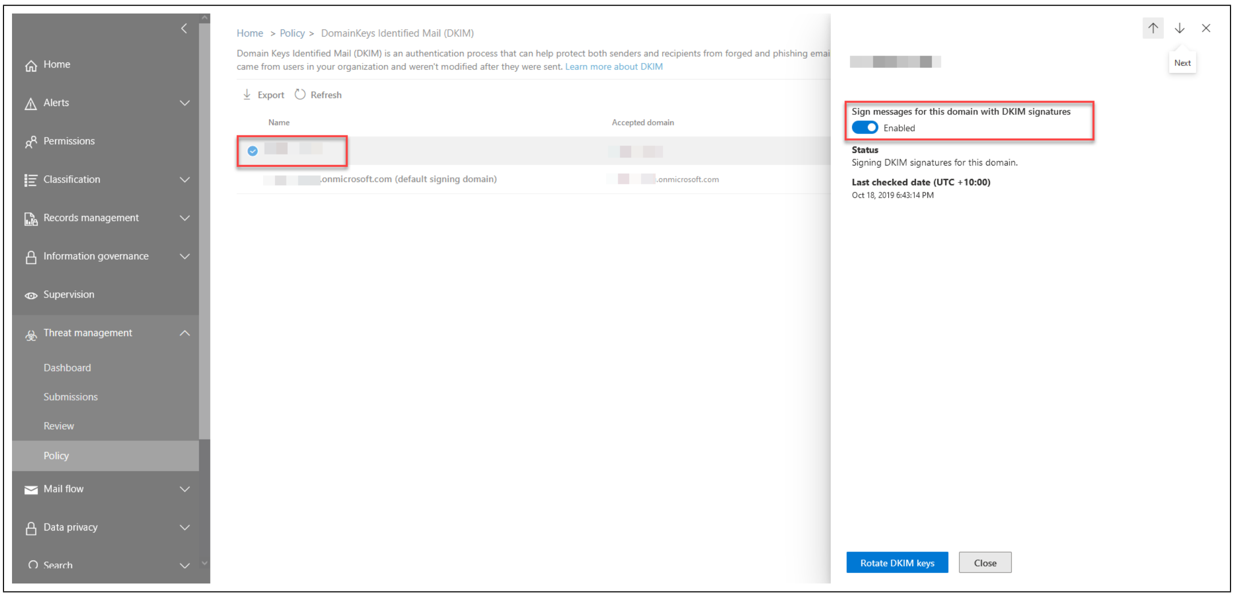
Login to Microsoft 365 Admin Center, then:

1. Select **Security**
2. Expand **Threat Management**, then select **Policy**, then select **DKIM**
3. Create a domain key when prompted to, and note down the DNS records that need to be created
4. Create 2 entries to the DNS records:

```
Name: selector1._domainkey
Type: CNAME
Value: (Value taken from Microsoft 365)
TTL: 3600
```

```
Name: selector2._domainkey
Type: CNAME
Value: (Value taken from Microsoft 365)
TTL: 3600
```

5. Wait for the DNS records to propagate (this usually takes about 1 hour, but can take longer)
6. Select each domain, one by one, and ensure **Sign messages for this domain with DKIM signatures** is set to **Enabled**



Home > Policy > DomainKeys Identified Mail (DKIM)

Domain Keys Identified Mail (DKIM) is an authentication process that can help protect both senders and recipients from forged and phishing emai came from users in your organization and weren't modified after they were sent. Learn more about DKIM

Name	Accepted domain
[redacted]	[redacted]
[redacted].onmicrosoft.com (default signing domain)	[redacted].onmicrosoft.com

[redacted]

Sign messages for this domain with DKIM signatures
● Enabled

Status
Signing DKIM signatures for this domain.

Last checked date (UTC +10:00)
Oct 18, 2019 6:43:14 PM

Figure 8: Enabling DKIM

Email bounce message is nondescript

Purpose

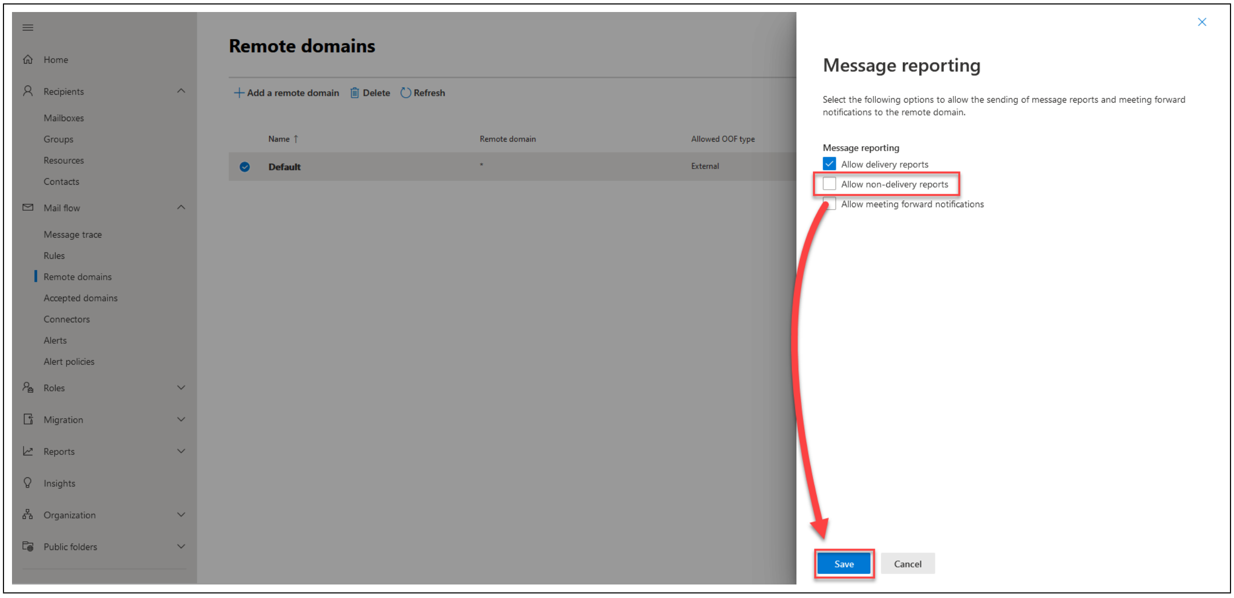
By default, Exchange Online will send a bounce response email if the sender specifies a **To** address that does not exist. This default bounce response contains information about the original email's spam score that can be used by attackers to continuously re-craft their phishing emails until the spam score is low enough that it is likely to land in victim's mailboxes.

Recommendation

By setting the bounce response message to something nondescript, or disabling it entirely, attackers cannot abuse it for phishing purposes.

Login to Microsoft 365 Admin Center, then:

1. Select **Exchange**
2. Expand **Mail flow**, then select **Remote domains**
3. Select **Default**, then select **Edit message reporting**
4. Ensure that **Allow non-delivery reports** is **Unchecked**
5. Select **Save**



Name ↑	Remote domain	Allowed OOF type
Default	*	External

Message reporting

Select the following options to allow the sending of message reports and meeting forward notifications to the remote domain.

Message reporting

☑ Allow delivery reports
□ Allow non-delivery reports
□ Allow meeting forward notifications

Figure 9: Disabling non-delivery reports

“onmicrosoft” email aliases removed

Purpose

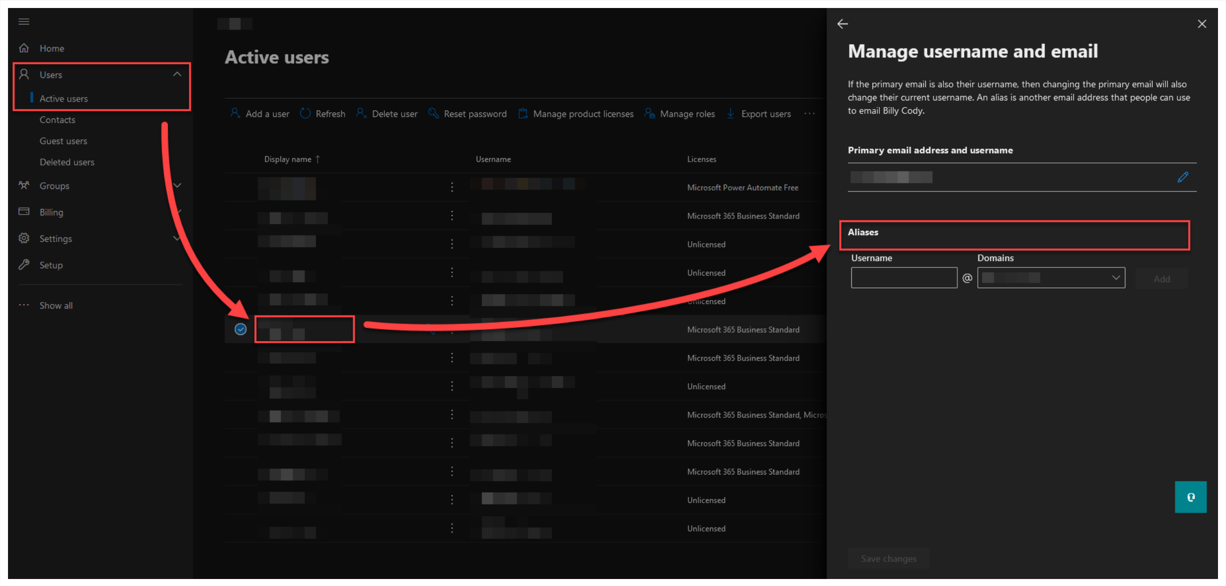
By default, when a new account is created it is automatically assigned an email alias, like **username@domain.onmicrosoft.com**. If Company Name uses an email filter solution or wishes to implement one later, attackers could potentially bypass that solution by sending email to the alias instead of the main email address.

Recommendation

Remove the email alias for all accounts.

Login to Microsoft 365 Admin Center, then:

1. Expand **Users**, then select **Active users**
2. Select each account, one by one, and choose **Manage username and email**
3. Ensure that the “onmicrosoft.com” email alias is not in the **Aliases** list. If it is, remove it.



Display name ↑	Username	Licenses
[redacted]	[redacted]	Microsoft Power Automate Free
[redacted]	[redacted]	Microsoft 365 Business Standard
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	nlicensed
[redacted]	[redacted]	Microsoft 365 Business Standard
[redacted]	[redacted]	Microsoft 365 Business Standard
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Microsoft 365 Business Standard, Micro
[redacted]	[redacted]	Microsoft 365 Business Standard
[redacted]	[redacted]	Microsoft 365 Business Standard
[redacted]	[redacted]	Unlicensed
[redacted]	[redacted]	Unlicensed

Manage username and email

If the primary email is also their username, then changing the primary email will also change their current username. An alias is another email address that people can use to email Billy Cody.

Primary email address and username

[redacted]

Aliases

Username: @ Domains: [redacted]

Figure 10: Removing onmicrosoft aliases

Calendars are not shared externally

Purpose

If an attacker gains access to a user's calendar, they could abuse the knowledge of meetings and appointments to target that user for further compromise. By protecting a user's calendar from being shared external to Company Name, this risk is mitigated.

Recommendation

Login to Microsoft 365 Admin Center, then:

1. Expand **Settings** then select **Org Settings**
2. Select **Calendar**
3. Ensure that **Let your users share their calendars with external users who have O365 or Exchange** is **Unchecked**
4. Select **Save**

Office add-ins restricted

Purpose

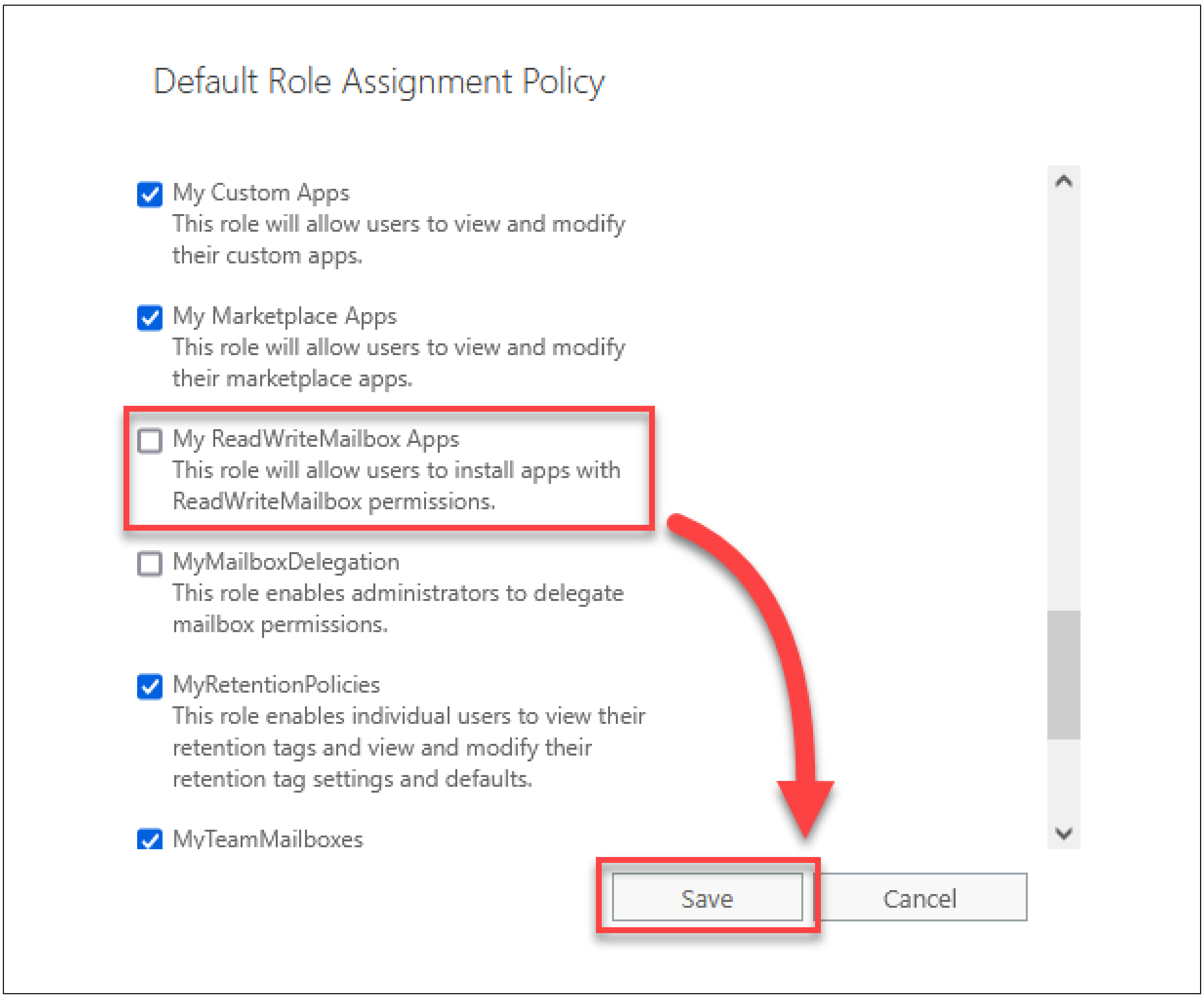
Add-ins are commonly used by attackers to gain access to sensitive information inside Office documents and emails. Restricting Add-ins if Company Name doesn't use them is an effective way to protect against malicious add-ins.

Recommendation

Office add-ins are disabled in 2 locations. One for Outlook add-ins and the other for document add-ins.

To disable Outlook add-ins, login to Microsoft 365 Admin Center, then:

1. Select **Exchange**, then select **Classic Exchange admin center**
2. Select **Permissions**, then select **User roles**
3. Edit the user role (by default it is **Default Role Assignment Policy**)
4. Ensure the **My ReadWriteMailbox Apps** checkbox is **Unchecked**
5. Select **Save**



Default Role Assignment Policy

☑ My Custom Apps
This role will allow users to view and modify their custom apps.

☑ My Marketplace Apps
This role will allow users to view and modify their marketplace apps.

□ My ReadWriteMailbox Apps
This role will allow users to install apps with ReadWriteMailbox permissions.

□ MyMailboxDelegation
This role enables administrators to delegate mailbox permissions.

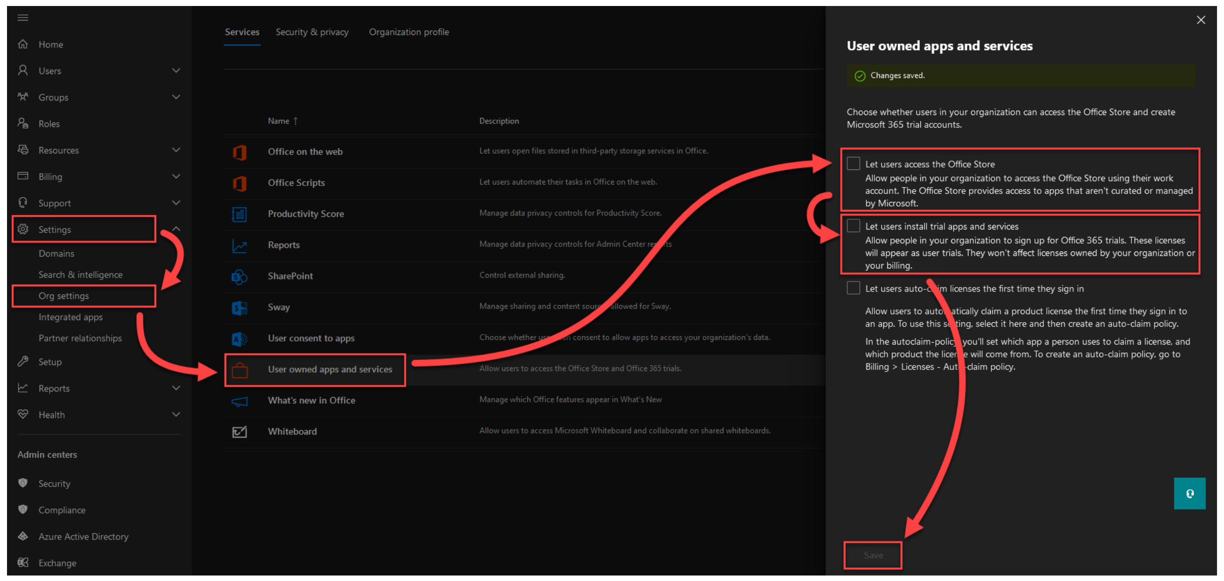
☑ MyRetentionPolicies
This role enables individual users to view their retention tags and view and modify their retention tag settings and defaults.

☑ MyTeamMailboxes

Figure 11: Disabling Outlook add-ins

To disable Office document add-ins, login to Microsoft 365 Admin Center, then:

1. Expand **Settings**, then select **Org Settings**
2. Under **Services**, select **User owned apps and services**
3. Ensure the **Let users access Office Store** and **Let users install trial apps and services** check-boxes are **Unchecked**
4. Select **Save**



Name ↑	Description
Office on the web	Let users open files stored in third-party storage services in Office.
Office Scripts	Let users automate their tasks in Office on the web.
Productivity Score	Manage data privacy controls for Productivity Score.
Reports	Manage data privacy controls for Admin Center reports
SharePoint	Control external sharing.
Sway	Manage sharing and content sources allowed for Sway.
User consent to apps	Choose whether users can consent to allow apps to access your organization's data.
User owned apps and services	Allow users to access the Office Store and Office 365 trials.
What's new in Office	Manage which Office features appear in What's New
Whiteboard	Allow users to access Microsoft Whiteboard and collaborate on shared whiteboards.

User owned apps and services

Changes saved.

Choose whether users in your organization can access the Office Store and create Microsoft 365 trial accounts.

☐ Let users access the Office Store
Allow people in your organization to access the Office Store using their work account. The Office Store provides access to apps that aren't curated or managed by Microsoft.

☐ Let users install trial apps and services
Allow people in your organization to sign up for Office 365 trials. These licenses will appear as user trials. They won't affect licenses owned by your organization or your billing.

☐ Let users auto-claim licenses the first time they sign in

Allow users to automatically claim a product license the first time they sign in to an app. To use this setting, select it here and then create an auto-claim policy.

In the autoclaim-policy, you'll set which app a person uses to claim a license, and which product the license will come from. To create an auto-claim policy, go to Billing > Licenses - Auto-claim policy.

Figure 12: Disabling Office document add-ins

DMARC Records are published

Purpose

Domain-based Message Authentication (DMARC) works together with SPF and DKIM to authenticate email senders and protect against phishing and other malicious emails. It may also be used to collect metrics about the emails being sent from your domain, such as when emails are perceived as spam or malicious. If malicious emails are coming from Company Name domains, it could be an indicator of account compromise.

Recommendation

Set a DMARC entry in the DNS records. The following is a baseline entry that will not return any metrics:

```
Name: _dmarc
Type: TXT
Value: v=DMARCv1; p=none;
TTL: 3600
```

For more details about DMARC and how to tune the record, refer to:

- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email

Appendices

Appendix A: Phishing campaign results

Note: Users with “Submitted Data” status were determined by correlation of IP address of the system that attempted to enter credentials and User ID assigned as part of the campaign. This correlation may not be accurate and should be interpreted as a best guess of the consultant.

First Name	Last Name	Status
John	Doe	Email/SMS Opened
Jane	Doe	Email/SMS Opened
John	Doe	Email/SMS Opened
Jane	Doe	Email/SMS Opened
John	Doe	Email/SMS Opened
Jane	Doe	Email/SMS Opened
John	Doe	Clicked Link

Appendix B: Security review methodology

Volkis will perform a review of the security posture of systems and services specified in the target scope. This will include an analysis of current configurations and integrations against a specified framework, standard or best practices, and recommendations for improvement based on our understanding of the client environment.

Assessing expectations

Before the security review can commence, Volkis will need to establish a baseline from which to compare against. The best place to start is by gaining an impression of how the client believes the system or service is configured, any integrations or compensating controls that may be in place, and what they wish to achieve through this report. Volkis prefers to do this in a interview or meeting format, but can be offered as a questionnaire in some cases.

Some examples of questions that may be asked are:

- What is the service used for?
- Does it integrate or connect with additional services?
- Does it have known insecure configurations for which compensating controls have been installed?
- Does it need to comply with a particular framework or standard?
- Does the client have additional security policies that the service needs to comply with?
- Are there any areas of concern that the consultant should focus efforts on?

Configuration

With the baseline established, the consultant will review the configuration of the service. The consultant will work systematically through the configuration sections, making note of insecure default options or non-standard insecure configurations. This can take the form of a checklist or a experience-based review depending on the client's requirements.

While the consultant may use a checklist to ensure all aspects of the review are covered, additional checks are made based on client requirements. If the client's policies or areas of concern address particular topics not covered by Volkis's standard review procedures, the consultant will research, develop and perform additional checks to meet that requirement.

Integration

As many applications integrate with services such as communications platforms, authentication platforms or file sharing platforms, a wholistic analysis of the client's security posture needs to be considered. Depending on the service, these integrations can offer security benefits, or present a security risk in themselves, and need to be evaluated accordingly.

In cases where a third-party security service has been integrated with application, some best-practice secure configurations may inhibit the service from operating correctly. As an example, secure authentication services such as SAML authentication or Single-Sign on (SSO) providers, work as a replacement for some of the applications authentication controls, such as Multi-Factor authentication. The consultant would need to consider this when reviewing the security posture of authentication mechanisms.

On the other side, some communications or file-sharing applications can bypass secure configurations, granting access to data the user should not have access to, presenting a security risk.

It is best to review all integrated services during the same engagement.

Analysis

When all checks are completed, the consultant will compare the results with the established baseline and requirements. Security integrations and compensating controls will be considered to determine the security posture of the client and areas of improvement. The consultant will create a report with all findings, their purpose, remediation steps and any additional points that will help to improve security of the service.

Appendix C: Web application penetration testing methodology

Volkis will perform penetration testing on the target web application. This will include the identification and enumeration of the application, identifying vulnerabilities, exploiting identified vulnerabilities, and then analysing and reporting on the results.

Our methodology is based on multiple industry recognised methodologies including OWASP.

Identification and enumeration

Volkis will investigate the application using scanning methods, active enumeration to identify packages, frameworks, and software in place, and Open Source Intelligence (OSINT). Volkis will also scan the web server as well, identifying other services hosted on the server that could be leveraged to compromise the application.

Volkis will scan the server using a port scanner, scanning for common TCP and UDP open ports. Where possible and if the server can handle the traffic throughput, full TCP port scans will be launched against the server. Any open services and ports will be enumerated to identify what service is running and information about that service including the version, banner information, and any third party plugins and modules that could be installed.

Spidering and web discovery tools will be run on the web application to identify all the different parts of the application, and to uncover hidden parts of the application. This may include running file and directory brute forcing attacks against the application. As part of this effort, a search for hidden assets and endpoints will be performed. This is to expand the attack surface and find things such as:

- Non-linked admin/high value pages;
- Websites behind a virtual hostname;
- UAT pages/instances with live data.

The application will then be profiled to identify standard packages, frameworks, and software used as part of the application. This will include identifying the web server and operating system, any development frameworks such as PHP or ASP.NET, any application frameworks such as Wordpress or Drupal, any Javascript libraries or frameworks such as Telerik or React.JS, and any user interface assistance libraries such as Bootstrap or JQuery.

The tester will investigate the organisation using common OSINT sources. This could include WHOIS information, social media sources and publicly available websites including the organisation's website. Other assets that may impact the security of the external network such as DNS, email, code repositories, third party hosting and Software as a Service providers will also be considered as part of the security posture.

Vulnerability identification

Each open system, service, page, form, and asset in the web application and on the web server will be investigated for potential vulnerabilities including, but not limited to, the OWASP Top 10 that could be used to compromise systems, gain access to information, make malicious changes to information or applications, or create impact on the availability of systems and information.

The network vulnerability identification will begin with using automated vulnerability assessment tools on the environment. This will include running generalist network vulnerability assessment tools such as Tenable Nessus that will scan for potential misconfigurations, missing patches, out-of-date software, and other common vulnerabilities. For specific services, more specialised vulnerability scanning and assessment tools will be used. These specific tools will give greater depth of vulnerability assessment than the general vulnerability assessment tools.

Web application scanning tools may also be used on the application. This may be generalist web application scanning for the entire site, or targeted scanning on specific pages, depending on the judgement of the tester. Due to the complexity of some applications, generalist scanners may either impact the availability of the application or may not be able to complete the scan in time, and so will be used with caution.

Following the vulnerability assessment, and with assistance of the results of the identification, enumeration, and vulnerability assessment results, the tester will then use manual techniques to uncover vulnerabilities that automated techniques will not see. This will include targeting custom developed services, leveraging the OSINT information, investigating the feedback that the services provide when test cases are entered, and other manual techniques.

Vulnerabilities that are identified will not just be technical vulnerabilities, but could also include logic flaws, gaps in business process, or any other weakness of the application that could present risk to the organisation.

Exploitation

The tester will exploit identified vulnerabilities to better understand its impact and to eliminate the possibility of a false-positive.

The exploitation will occur alongside the vulnerability identification phase as vulnerabilities are identified. It will incorporate prioritisation, where vulnerabilities that tend to present higher risk to the organisation will be prioritised over low risk vulnerabilities. If there is a significant chance of service disruption, the tester will organise a window for exploitation, or not exploit it at all.

Exploitation will often involve the usage of publicly available tools, custom written tools, or specific actions taken by the tester.

Due to the nature of certain vulnerabilities, not every vulnerability can be exploited by the tester. This could be due to the level of network or system access required for exploitation, privilege requirements for exploitation, or specific conditions that need to be in place. These vulnerabilities will still be reported on even if exploitation was not achieved. The lack of exploitation will be a consideration when assessing the risk rating during the risk assessment.

Due to time limitations and prioritisation, not all vulnerabilities that are identified will be exploited during this phase. For example, the tester may choose not to exploit vulnerabilities that present a low risk to the organisation or that have a known impact.

Sensible precautions will be used during the exploitation phase to minimise the risks of availability issues. This could include performing exploitation out-of-hours or using a development or testing server. If the risks of exploitation are considered greater than the benefit of exploitation, and those risks cannot be mitigated or managed, the exploitation of the vulnerability will be skipped.

Exploitation of vulnerabilities that specifically create Denial of Service (DoS) condition will not be performed, nor will any sort of Distributed Denial of Service (DDoS).

Post-exploitation

Successful exploitation of vulnerabilities will provide the tester with additional access to information, functionality, and potential access to the internal environment. This additional access will be used by the tester to determine and prove the full scope of compromise, including the true business impact of the vulnerability.

The additional access will be fed back into the previous stages to determine if additional services can be enumerated and additional vulnerabilities can be found and exploited.

Appendix D: Risk assessment methodology

A qualitative risk assessment is performed on each vulnerability to determine the impact and likelihood of the vulnerability being exploited. An overall risk is calculated based on the table below:

Likelihood Impact	Rare	Unlikely	Possible	Likely
Critical	**Medium**	**High**	**Critical**	**Critical**
Severe	**Low**	**Medium**	**High**	**High**
Moderate	**Low**	**Medium**	**Medium**	**High**
Low	**Low**	**Low**	**Low**	**Medium**

The risk assessment methodology is derived from industry standards such as ISO 31000[1] and OWASP Risk Rating Methodology[2].

The impact rating is deduced from multiple factors that consider both technical impact and business impact:

- **Loss of confidentiality**: How much sensitive information could be accessed or leaked and how sensitive was it?
- **Loss of integrity**: How much data could be corrupted and what degree of corruption was possible? Was it possible to perform actions on behalf of others?
- **Loss of availability**: How much services could be disrupted, preventing users from performing their tasks? What was the degree of impairment?
- **Financial damage**: How much money could be lost as a result?
- **Reputational damage**: How badly would the company's reputation be damaged and how much trust could customers lose?
- **Non-compliance**: Would the business be in breach of certain compliance standards they are obliged to comply with? (E.g. Privacy Act)

The likelihood is deduced from considering who the adversary may be and factors around the vulnerability:

- **Skill of adversary**: How skilful is the attacker likely to be?
- **Motive**: What are the motivating factors that the adversary may have?
- **Resources**: How much time and economic resources does the adversary have?
- **Ease of discovery**: How likely is the adversary to discover the vulnerability?
- **Ease of exploitation**: How easy is the vulnerability to exploit and are there publicly available tools to aid in doing so?

[1] https://www.iso.org/iso-31000-risk-management.html
[2] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

- **Detection**: How likely is the attack to be discovered by the organisation?

An overall rating (from Low to Critical) is given to each vulnerability. The vulnerabilities are then sorted in order from importance and urgency to remediate.

Appendix E: Document control

Document information

Client	Company Name
Document name	Security Review & Phishing Campaign
Document version	1.0

Document changes

Version	Date	Name	Changes
0.1	2023-01-01	Contributor #1	Initial Draft
1.0	2023-01-02	Contributor #1	Release to client

Document contributors

Name	Role	Phone number	Email address
Contributor #1	Security Consultant	Ph #1	Email #1
Contributor #2	Security Consultant	Ph #2	Email #2

VOLKIS™