Protection against Microsoft Office 365 credential phishing and data breaches

Contents

Foreword

Especially during the first half of 2018, more and more cases were reported to the National Cyber Security Centre Finland (NCSC-FI) in which organisations were subject to phishing with the purpose of obtaining the email credentials of employees. Phishing can target both regular people and organisations. Data breaches targeting business accounts are usually referred to as business email compromise (BEC).

User credentials can be used in many ways, depending on the criminal's personal motives or the role or position of the breached user account in the organisation. For example, in certain cases, the attacker was clearly seeking significant financial gains by monitoring payment-related messages. On the other hand, stolen credentials can also be used, for example, to acquire business secrets. In addition, successful phishing may involve different reputation and regulatory risks.

Although phishing as a phenomenon is not only limited to the services of specific providers, what these cases had in common was that the captured credentials were expressly related to Microsoft Office 365 accounts. Similar cases are constantly being reported to NCSC-FI. NCSC-FI published a credential phishing alert in June 2018, and it remains valid at the time of writing.

We have seen a number of different development paths in phishing campaigns since late spring and early summer. This partly explains the persistence of this phenomenon. Individual examples include phishing messages that resemble encrypted emails, the bypass of multi-factor authentication using former email connection methods and the customisation of the phishing site layout, depending on the email service from which each user accesses the service.

Reacting to new phishing campaigns is a never-ending race and is unfortunately often too late after the wave has already hit the shore. This is why it is very important to use service-specific information security features as early as possible. Different means can be used to reduce the number of phishing messages that reach users, prevent the easy use of stolen credentials, investigate possible cases and restrict the impact of successful phishing.

This guide focuses on the protection of Microsoft products, because they have been involved in several campaigns targeted especially at companies reported to NCSC-FI during the past year. In addition, NCSC-FI has discovered that companies often face problems in the deployment of the security features and settings of these products.

We hope that this guide helps organisations to strengthen their email and cloud service environments, especially against threats related to credential phishing. The guide assumes that the reader has a basic knowledge of Microsoft's cloud services.

Abstract

In recent years, we have often read that usernames and passwords have fallen into the wrong hands. News have mostly concerned about risks associated with the user databases of different services. Consumers using the same passwords in different services have given cybercriminals an opportunity to use stolen credentials in other services.

The use of cloud services has spread rapidly among organisations. Microsoft Office 365 is used widely in Finland in both the private and public sectors. Identities used in Office 365 are stored and maintained in the Azure Active Directory (Azure AD) service. Many other cloud services can often be used with these same credentials.

Phishing is one of the most common information security threats. According to the annual "Information Security in 2018" review issued by NCSC-FI in February 2019, the most significant information security threat in 2018 comprised the gradually spreading Office 365 phishing campaigns aimed at stealing user credentials.

Office 365 and many other Microsoft cloud services include various features that help to significantly reduce the success of phishing. These services can be purchased as different customised versions, i.e. subscriptions. These subscriptions include a pre-defined number of licences that each organisation's ICT administrators allocate to users. Organisations can

acquire identical licences for all users or separate licences for employees in different roles.

Features available to prevent phishing depend on the subscriptions used. This document presents protection methods that do not depend on the subscriptions or licences organisations use.

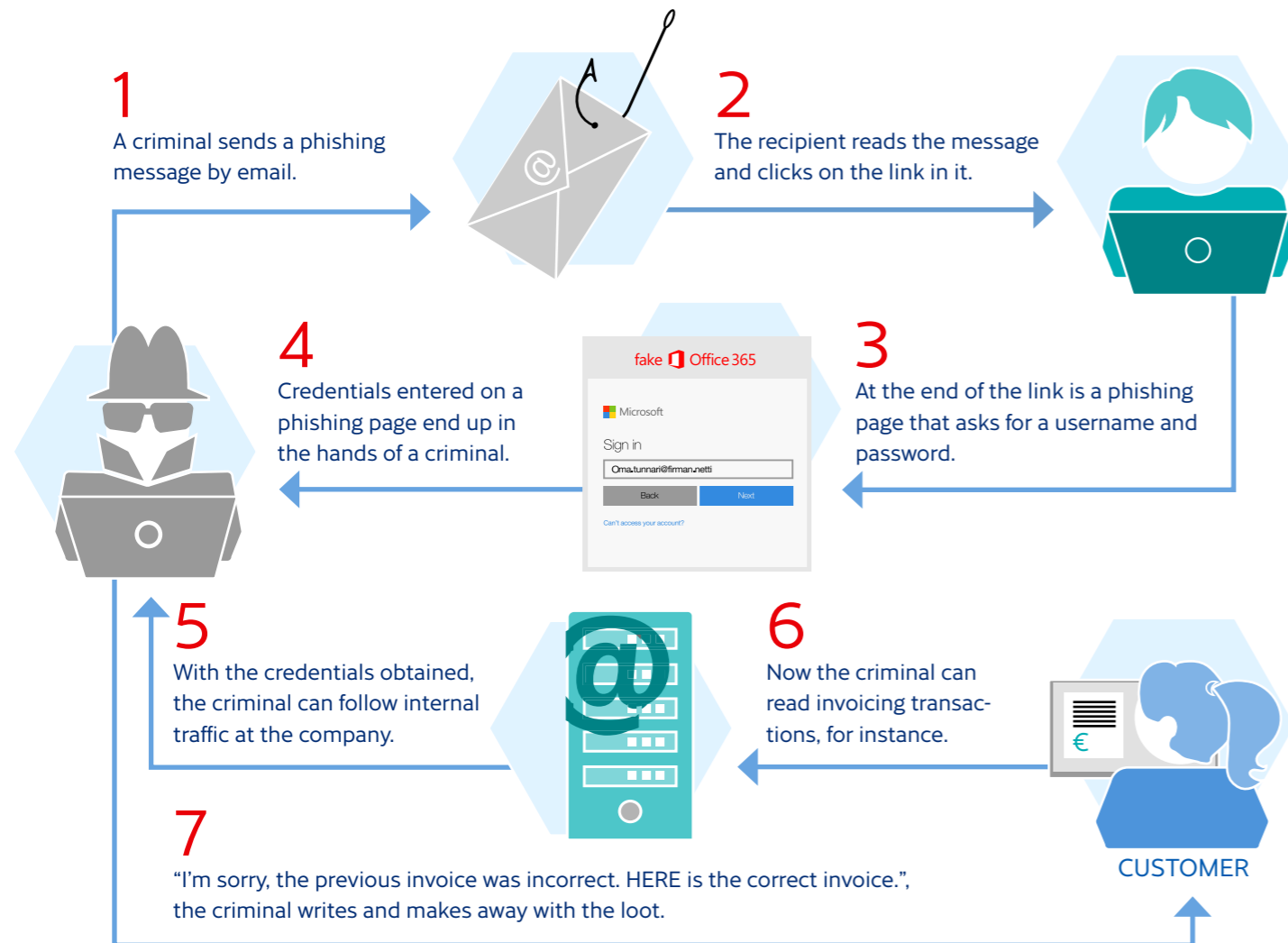The most important ways to prevent phishing, regardless of subscriptions and licences, are:

1. Deployment and enforcement of modern authentication
2. Deployment of two-factor authentication
3. Ensuring the quality, quantity and retention period of logs.

1 Why is the protection needed?

Information security consists of a number of different areas. This document focuses on mitigating phishing.

Phishing can be done in many ways. In the broadest sense, phishing messages are sent to large groups of users. The aim of targeted phishing is to steal credentials saved in an organisation's cloud services and/or the credentials of IT administrators. Attacks can also target business managers or other employees who process financial transactions and invoices.

1
A criminal sends a phishing message by email.

2
The recipient reads the message and clicks on the link in it.

4
Credentials entered on a phishing page end up in the hands of a criminal.

fake Office 365

Microsoft
Sign in
Omastunnari@firman.netti
Back | Next
Can't access your account?

3
At the end of the link is a phishing page that asks for a username and password.

5
With the credentials obtained, the criminal can follow internal traffic at the company.

6
Now the criminal can read invoicing transactions, for instance.

CUSTOMER

7
"I'm sorry, the previous invoice was incorrect. HERE is the correct invoice.", the criminal writes and makes away with the loot.

1.1 Criminals often aim to create fake invoices

Nowadays, phishing is done by several different groups of criminals. These groups differ in competence levels and typically use slightly different tools to meet various purposes. At least two different operating methods have been identified:

- Most often, criminals aim to capture as many email credentials as possible. They log in to accounts to find search words related to invoicing. This information is then used to prepare fake invoices using the details and context of real invoices. If an account is not interesting, criminals use it to send phishing messages to the victim's contacts.
- In rarer cases, criminals aim to monitor messages sent to and from an inbox to obtain information. NCSC-FI has received information about cases in which inboxes of key employees have been hacked to monitor the exchange of messages. Criminals then forward messages to one of their own inboxes. The exact motive of such criminals has not been identified.

1.2 Criminals can bypass two-factor authentication

Different groups of criminals have slightly different technical skills. However, these differences are no longer particularly distinctive, and most groups are able to bypass two-factor authentication, for example. This has been done in at least two different ways:

- Typically, criminals use a feature of Office 365, which allows hardware and software that do not support two-factor authentication to log in to services. Currently, this legacy authentication mode, is broadly used by criminals. This guide instructs readers to implement modern authentication and prevent legacy authentication based logins.
- Criminals use a stolen username and password to log in to a service, and the victim receives a genuine verification code, for example, by a SMS. When the user accesses the phishing site, they are also asked to enter this second factor authentication code, allowing criminals to log in to the actual service.

1.3 Example cases from the National Bureau of Investigation of Office 365 data breaches

Finnish police consider phishing to be alarming. Phishing is mainly done using skilfully crafted phishing sites. After accessing the Office 365 service of companies, criminals may spend a great deal of time monitoring emails. On the other hand, not many offences are reported to police, due to which police cannot gather sufficient intelligence to identify the criminals.

> **Financial company A**
> The company's Office 365 cloud service was hacked by means of phishing. Messages containing a link to a phishing site were sent to two of the company's employees. The criminals monitored the company's emails for several months and made changes to email forwarding without the company knowing. Financial company A did not know how long its emails had been monitored or what information had potentially leaked. In addition, the criminals tried to use fake invoices to make the company transfer funds to their account. The criminals used information obtained from monitored emails to prepare these fake invoices, attempting to make the invoices look as real as possible.

> **Industrial company B**
> The company's Office 365 cloud service was hacked by means of phishing, just as in the example above. Phishing links were sent from the company's email system to people working in the company's subsidiaries and its subcontractors and customers. The company noticed that unauthorised forwarding rules had been added to its email system. Unfortunately for the police, the data breach in the company's system was discovered so late that log data about the breach was no longer available.

2 Office 365 from the perspective of phishing

Microsoft Office 365 is a cloud service which is also widely used in Finland. Its key components include Exchange Online, SharePoint Online and Teams. Skype for Business Online will be excluded from the service, as similar messaging features are available in Teams. Most Office 365 licences also include desktop solutions for knowledge work, such as Outlook, Word, Excel and PowerPoint.

Enterprise Mobility + Security (EMS) offers knowledge work management and information security services in a single solution. It includes more comprehensive versions of Azure AD, Intune device management service, and Azure Information Protection for the protection of data.

Microsoft 365[1] combines Office 365 with Windows 10 and EMS.

Phishing is usually done via email, and its goal is to steal usernames and passwords. This is why Exchange and Azure AD, which is used to authenticate users, are key Office 365 services in terms of phishing. By improving their security level, phishing can be mitigated or at least the likelihood of its success significantly reduced.

Phishers can present user SharePoint sites, for example. As these are not genuine or produced by the organisation, protecting the organisation's SharePoint service does not help.

If phishing is successful and criminals are able to steal passwords, their traces may remain in email and sign-in logs, as well as in the logs of other services. This will be discussed in more detail in the "Protection measures" section.

[1] https://www.microsoft.com/fi-FI/microsoft-365/

2.1 Office 365 versions

Office 365 is available as the Business version for organisations of a maximum of 300 people, and the Enterprise version for larger organisations. The latter[2] is also available at levels E1, E3 and E5. In addition, Office 365 comes as consumer and education/academic versions (Education A1, A3 and A5).

Office 365 can be acquired separately or as part of Microsoft 365. Microsoft 365 is also available as smaller (E3) and larger versions (E5).

Users log in to Office 365 services using Azure AD.

Its basic level is always included in Office 365. However, the more comprehensive Premium level (P1 or P2) is available as part of EMS, and therefore as part of Microsoft 365. In addition, Microsoft 365 is available as Microsoft 365 Firstline 1[3], including Azure AD Premium P1, among others.

All the options are illustrated in the following table. Office 365 Business is presented in a separate column. However, as stated above, Office 365 Enterprise can also be acquired separately.

Area	Office 365 Business only	Microsoft 365 E3	Microsoft 365 E5
Office 365	Business	Enterprise E3	Enterprise E5
EMS	– –	EMS E3, with Azure AD P1 + other	EMS E5 with Azure AD P2 + other
Windows 10		Enterprise	Enterprise + Windows Defender Advanced Threat Protection

It is also possible to combine subscriptions and their licences. For example, an administrator could have the Microsoft 365 F1 licence, plus the Azure AD P2 licence to use the Privileged Identity Management feature.

Since February 2019, it has been possible to acquire additional Identity & Threat Protection and

Information Protection & Compliance packages that include new information security features on top of the Microsoft 365 E3 subscription. As their names indicate, the former includes key services for identity management. Diagrams of different service packages and their features are available, for example, at https://github.com/AaronDinnage/Licensing

2 https://products.office.com/en-us/business/compare-more-office-365-for-business-plans
3 https://www.microsoft.com/en-us/microsoft-365/compare-all-microsoft-365-plans

2.2 Identity (Azure Active Directory)

Azure Active Directory is an identity management service, which is used by more than one billion users in tens of millions of organisations. Some of these are Office 365 users, while some use Azure AD for other applications. Different organisations and their users and data have been logically divided into tenants, which are isolated from one another[4].

Azure AD uses two different identity types: cloud (managed) and federated identities. In the former type, users are always authenticated using Azure AD. In the latter, users are authenticated outside Azure AD and, based on trust, Azure AD accepts the authentication performed by the external party. The identity type is domain-specific (email domain).

Hundreds of thousands of applications have been integrated with Azure AD. These do not require any separate login: it is sufficient that the user logs in to Azure AD. Permissions for these applications can be based on Azure AD user groups.

Azure AD can be connected with Active Directory Domain Services (AD DS) located in an organisation's own network (on-premises). AD DS is often referred to as Active Directory or AD. Integration enables a single set of credentials to be used in internal network and cloud services. Integrating is usually done by Azure Active Directory Connect, installed on the on-premises server.

In an integrated environment, users log in using any of the following methods[5]:

1. Password hashes are synchronised to Azure AD. (Password Hash Synchronisation, PHS)[6]. When using cloud services, authentication is performed by Azure AD.

2. Federated authentication: identities are sychronised, but password hashes are not. When users log in to a cloud service, they are forwarded to

Active Directory Federation Service (AD FS) in the on-premises environment. This solution often requires the use of four servers (two internal network servers and two DMZ servers). Authentication is performed by AD domain controller servers.

3. Passthrough Authentication (PTA) is used in the on-premises environment. This solution can be used to replace AD FS if an organisation has no other services in place using AD FS.

4. PingFederate[7] is used in the on-premises environment, and verification is performed by PingFederate.

Even if the organisation uses federated authentication (option 2 in the list above), password hashes can also be synchronised to Azure AD (option 1). This produces two types of benefits:
a) a quicker transfer to the cloud identity in place of a federated identity if there is a fault in the on-premises federation service
b) identification of credentials that have fallen into the wrong hands (Azure AD leaked credentials report[8]).

Azure AD also includes self-service password reset feature. In a cloud service, the password of a reset synchronised user can be synchronised to on-premises AD. This functionality requires Azure AD Premium (P1 or P2).

Considering the comprehensive maintenance of identities and protection against phishing, the key features of Azure AD are:

4 https://aka.ms/Office365TI
5 https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn
6 https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization
7 https://docs.pingidentity.com/bundle/O365IG2O_sm_integrationGuide/page/O365IG_c_integrationGuide.html
8 https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Azure-Active-Directory-Premium-reporting-now-detects-leaked/ba-p/249200

Multi-Factor Authentication (MFA)

MFA enables additional authentication in addition to the conventional username and password combination. Options for additional authentication are:
- one-time numerical code by telephone
- one-time numerical code by SMS
- approval using a mobile app (Microsoft Authenticator)
- one-time numerical code using a mobile app (Microsoft Authenticator).

Microsoft's cloud-based MFA is available in three different versions:
1. Multi-Factor Authentication for Office 365. This is a basic version included in Office 365, which can only protect Office 365 apps. In this version, the MFA requirement must be activated individually for each user.

2. Azure Multi-Factor Authentication. Azure AD Premium (P1 or P2) permits the activation of the MFA requirement using conditional access or separately for each user. Authentication is done using Azure MFA, or a separate authentication server can be installed in the organisation's network.
Note: Until September 2018, Azure MFA was available with a separate licence, but it is now only available with the Azure AD Premium subscription.

3. MFA for Azure Active Directory Global Administrators. Originally, MFA was only available for users with the Global administrator role in Azure AD. Later, the service was expanded to cover all users. In 2018, Microsoft made MFA for Global Administrators available using a baseline conditional access policy. Microsoft will activate the policy when it is officially released, i.e. when it reaches the general availability (GA) stage.

Conditional Access

Conditional access permits or prevents the use of cloud services (e.g. Office 365, Exchange Online) when certain conditions are met. For example, access can be permitted for a specific combination of a user location, device, service and authentication method.

Typically, a username and password combination is permitted in an internal network, while two-factor authentication is required in the public network. Another typical example is that services can only be used with an organisation's own devices. In this case, Office 365 services cannot be accessed from home computers.

Azure Active Directory Conditional Access is available in Azure AD Premium subscriptions.

The figure below presents the default policies of Windows Server 2019 AD FS.
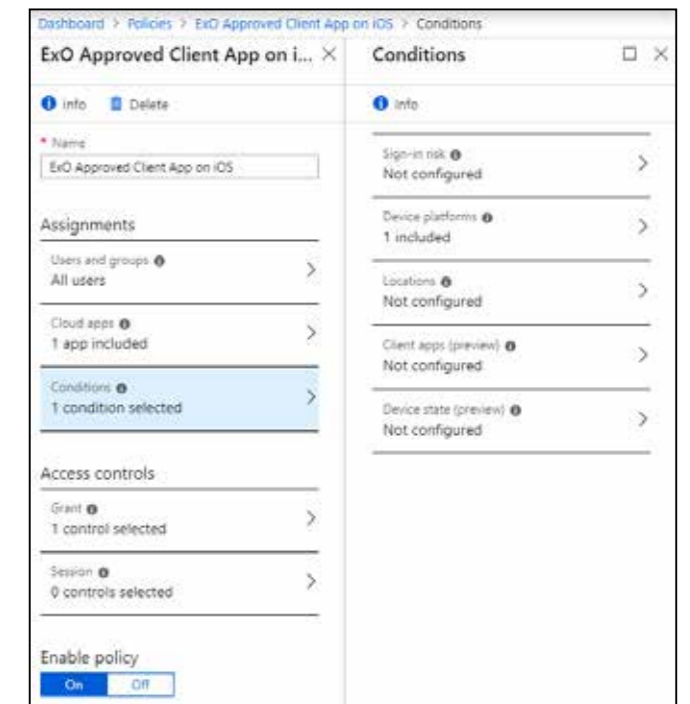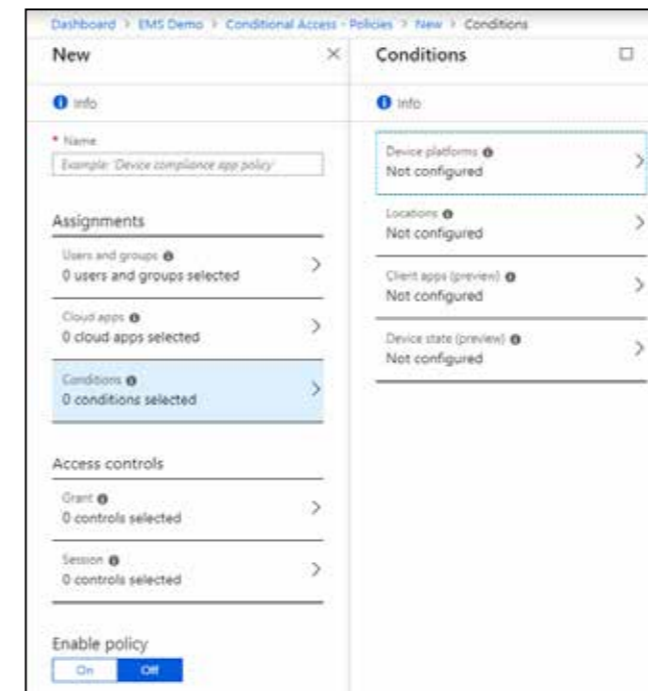
If Azure AD Premium licences are not used, similar functionality can be implemented using a federated identity in Microsoft AD FS. AD FS is a role included in Windows server operating systems. The figure above presents the default policies of Windows Server 2019 AD FS.
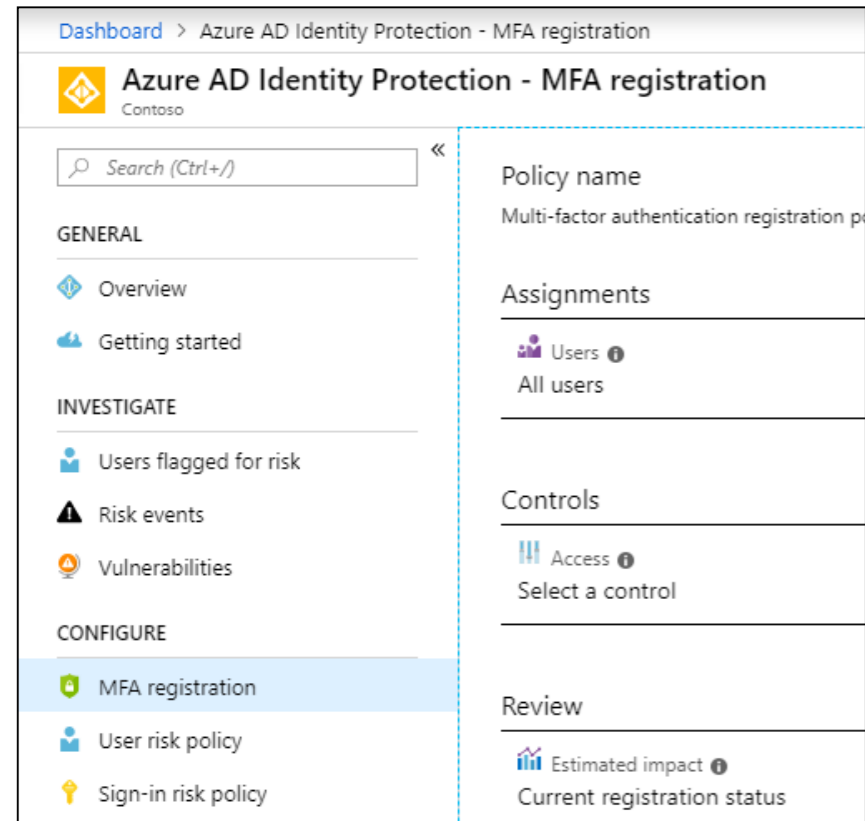
Identity Protection[9]

Identity Protection enables the following:
1. Identification of vulnerabilities that affect an organisation's identities
2. Automatic operation regarding suspicious events related to identities
3. Forensics and investigation of suspicious events.

Identity Protection also includes the MFA Registration feature, which can force users to register as MFA users.

New features were added to Identity Protection in January 2019[10].

Azure Active Directory Privileged Identity Management[11]

Using Privileged Identity Management, membership of Azure AD and Azure privileged roles can finally be controlled so that administrator roles are flexible. The number of permanent administrators can be reduced in most cases. Users activate their roles and related authorisation as required, and use can be audited. Roles can be activated using an approval procedure, in which case promotion to the role of administrator requires the approval of designated persons. These features are presented in the following table:
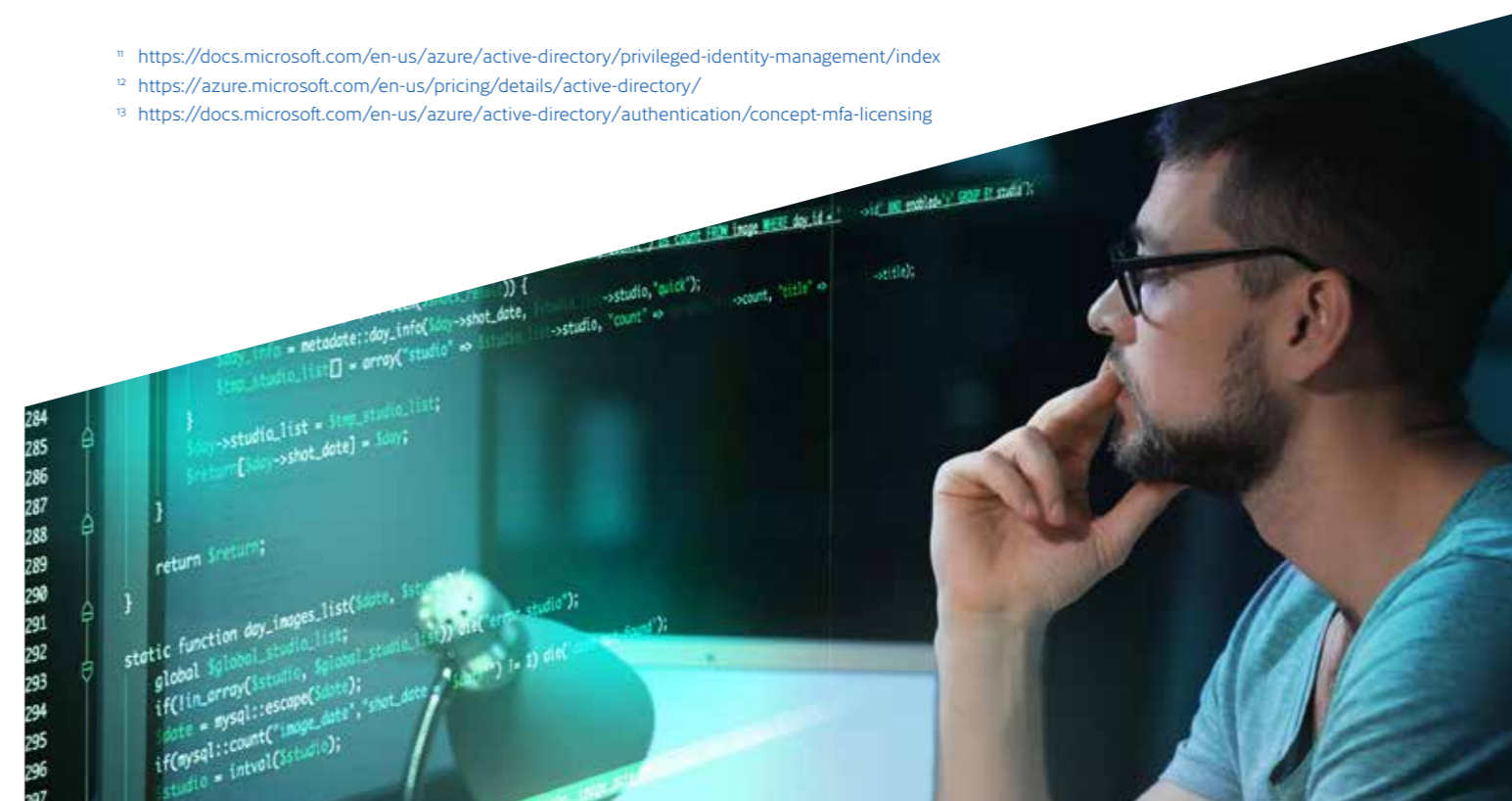
		Azure AD-version		
Function		Basic and Office 365	Azure AD P1	Azure AD P2
Multi-Factor Authentication for Office 365		X	X	X
Azure Multi-Factor Authentication			X	X
Conditional Access	Based on the device's operating system, location, application used or status		X	X
	Based on risks			X
Identity Protection				X
Privileged Identity Management				X

The different Azure AD versions and their features are presented in more detail on the Azure AD service pricing page[12]. Features of the different MFA versions are presented on a separate page[13].

9 https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/index
10 https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Four-major-Azure-AD-Identity-Protection-enhancements-are-now-in/ba-p/326935

11 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/index
12 https://azure.microsoft.com/en-us/pricing/details/active-directory/
13 https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

2.3 Email protection methods

Email can be protected by various technical means. Messaging between email servers can be encrypted using the Transport Layer Security (TLS) protocol. As TLS is based on certificates, it is also possible to verify the identity of the other party.

Different methods are also available for the prevention of junk mail. The methods presented in the following table help to prevent emails sent from the Office 365 environment being labelled as junk mail. These methods have no impact on incoming emails, as the sending party always defines settings.

	SPF	DKIM	DMARC
What does it mean?	Sender Policy Framework	DomainKeys Identified Email	Domain-Based Message Authentication, Reporting, and Conformance
What is it?	A system which determines and verifies who can send email from a specific domain.	An email authentication system based on asymmetrical encryption keys.	An email authentication system which helps to define what to do if a message does not pass the SPF or DKIM check.
How does it work?	The receiving party checks whether the sending party has the right to send an email using the specific domain. This information is saved in the TXT record of the specifid domain's DNS server.	The sending party signs the email and/or subject. The receiving party checks the signature and ensures that no data has been changed. A public key is released in the TXT record of the specific domain's DNS.	The receiving party carries out the SPF and DKIM checks. If the check fails, the receiving party will check the sending party's DMARC policy and decide what to do: reject the message, place it in quarantine or send it normally; additionally a report to the sender organisation can be sent.
Why is this important?	It reduces the likelihood of labelling outgoing messages as junk mail.	It significantly reduces the likelihood of labelling outgoing messages as junk mail.	It helps the receiving organisation to decide what to do with messages that do not pass the checks. It also acts as a feedback channel for the sender.

2.4 Sharing data in different services

In Office 365, files can be shared outside the organisation to enable and make collaboration more productive.

Sharing takes place, above all, in SharePoint document libraries directly using SharePoint features, Teams, or OneDrive for Business.

External users' access to the organisation's documents can also be defined as follows:
- Azure AD. A basic identity and authentication service.
- SharePoint Online and OneDrive for Business. OneDrive for Business also technically runs on SharePoint document libraries.
- Office 365 Groups. These groups can be used for permissions and group messaging.

- Each team runs on top of Office 365 Groups and the Sharepoint document library.

More information about the external users and their access to documents in Teams[15] is available through the link in the footnote.

To monitor the use of data stored in Office 365 and of other cloud services and for protecting data, Microsoft offers a Cloud Access Security Broker (CASB) solution called Cloud App Security[16]. It helps to:
- monitor the cloud services used by the organisation and associated risks
- protect data by monitoring and controlling the use of cloud services
- identify any irregular activities and information

security breaches, and react to them automatically; this can, for example, be done after successful phishing when files are sent to external users in a cloud service using stolen credentials.

The service is available in two versions[17]: Office 365 Cloud App Security and Microsoft Cloud App Security. The former is included in Office 365 E5, and the latter in EMS E5.

2.5 Information security architecture

The information security architecture of Azure AD differs significantly from that of the conventional Active Directory. The following table presents some differences between Active Directory Domain Service integrated with the Windows Server operating system and Azure AD.

	Active Directory (Domain Services)	Azure Active Directory
Purpose	An online on-premises operating system for Windows computers	Identity as a Service (IDaaS)
Certification	Kerberos and NTLM	OpenID Connect Security Assertion Markup Language (SAML), WS-Federation, ADAL
Authorisation	Operating system services	OAuth2
Retrieval of data	LDAP	REST API over HTTP or HTTPS
Management limits	Forest, tree, domain	Tenant
Access	Mainly from the internal network; certain functions (e.g. certification) also available from an external network via other services	From anywhere
Integration between organisations	Difficult	Easy

Azure Active Directory Domain Services[18] is available as a Microsoft identity service. It is a smaller version of conventional AD. Its main purpose is to offer AD services (authentication, retrieval and group policy) for services running on virtual servers migrated to Azure.

2.5.1 Azure AD access control model

Azure AD uses role-based access control (RBAC). There are many different roles, with Global administrator having the most extensive rights. Only users with this role have the right to assign administrator rights to other users and add new domains, for example. Users have the most limited rights. This role is automatically assigned to all users of Azure AD. User administrator role is sufficient for daily user management such as licence management and password resets.

Azure AD uses security groups familiar from Active Directory. These groups can, for example, be used for authorization in SharePoint Online. Unlike Active Directory, RBAC roles cannot be assigned to groups in Azure AD. If Azure AD is integrated with Active Directory, groups can be controlled in Active Directory.

When the security features of Azure AD are used, access in emergency situations must be ensured. Microsoft has prepared a guide[19] on how to prepare for different disruptive scenarios.

[14] https://blogs.technet.microsoft.com/fasttracktips/2016/07/16/spf-dkim-dmarc-and-exchange-online/
[15] https://docs.microsoft.com/en-us/microsoftteams/teams-dependencies
[16] https://docs.microsoft.com/en-us/cloud-app-security/

[17] https://docs.microsoft.com/en-us/cloud-app-security/editions-cloud-app-security-o365
[18] https://docs.microsoft.com/en-us/azure/active-directory-domain-services/
[19] https://aka.ms/resilientaad
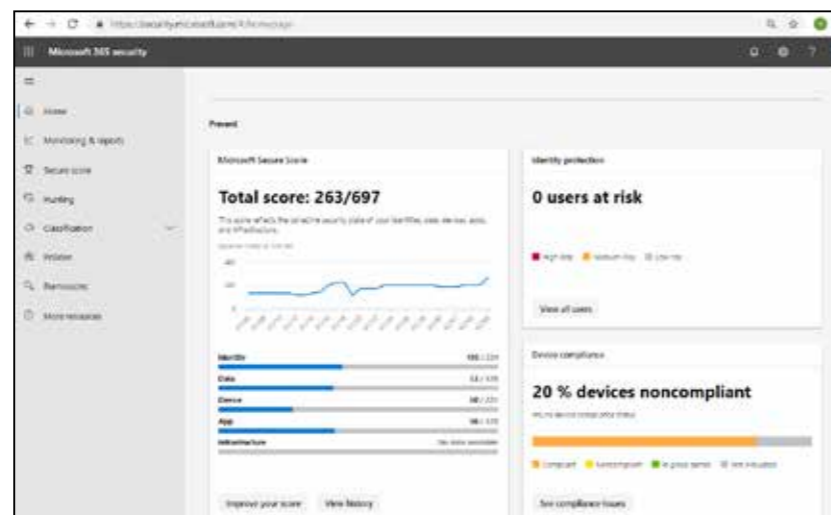
2.6 Microsoft Secure Score

Microsoft Office 365 Secure Score[20] was released in 2018. It provides administrators with an analysis of the current status of Office 365 information security and recommendations for actions to improve the status. These recommendations include descriptions of the threats against which the recommended actions provide protection. The impact of these actions on users and the complexity of deployment are also described.
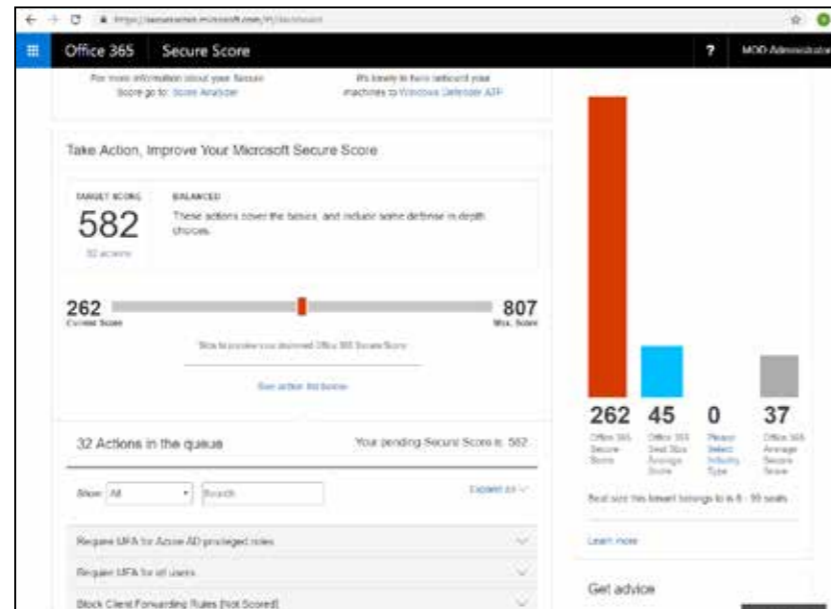
Identity Secure Score became available in 2018. It can be used as part of the Azure AD management portal.
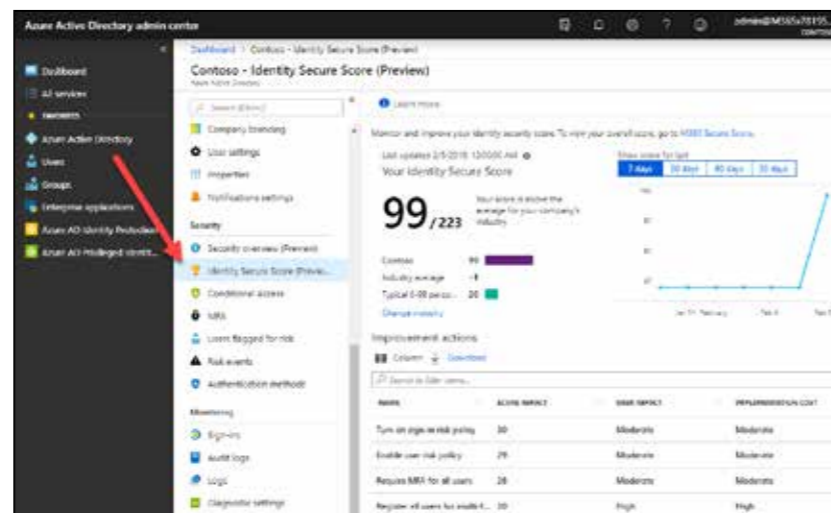
In January 2019, Microsoft released new Microsoft 365 Security Center and Compliance Center portals[21]. They are available in Microsoft 365 E3 and E5 subscriptions. In the Security Center portal, Secure Score has been divided into separate sections. For example, the tool includes forensics features. Security Center portal aggregates information from different sources.

[20] https://securescore.microsoft.com/
[21] https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Introducing-the-new-Microsoft-365-security-center-and-Microsoft/ba-p/326959

3   Protection measures

Technical debt may have accumulated in the services of organisations over the years, as the environments have not been kept up-to-date. A good example is the Windows 7 operating system, which is still widely used. At the time it was designed, modern threats were not present and thus were not taken in to account.

3.1   Securing identities

Securing identities is the most important security area. Because services located in any cloud can be used on different devices from any location, conventional protection is no longer enough.

3.1.1   Customise login pages to match your organisation's look

Office 365 login pages can be customised according to the look of each organisation[22]. This helps users familiarise themselves with the organisation's look and makes phishing more difficult when using fake login pages.

However, users cannot fully rely on the appearance of a page. After all, cybercriminals may have made a completely identical fake page. In this case as well, the fake page can be identified based on the URL and certificate.

3.1.2   Protect passwords

It is important to ensure that passwords are sufficiently complicated and long. This helps to reduce the likelihood of guessing passwords. However, complexity does not help if a user enters their strong password on a fake phishing site. The prevention of commonly used passwords is now possible in Azure AD and in the on-premises Active Directory[23]. Limiting passwords in on-premises environments using this feature requires Azure AD Premium licences.

Cloud services are updated as frequently as once a week. As such, it is difficult for administrators and service desks to keep up.

When these two realities meet, the result may be a complicated deployment project.

There are many ways to prevent passwords from being cracked by guesswork or brute force. Microsoft has released recommendations on what to do to prevent passwords from being guessed or cracked[24].

If federated authentication is used, Extranet Lockout[25] should be enabled. This feature became available in the Windows Server 2012 R2 version, and it has been developed further in later operating systems (Windows Server 2016 and 2019).

3.1.3 Secure Active Directory

In an environment synchronized with Azure AD, in particular, the management of local Active Directory is also important.

Active Directory was released in 2000 as integrated with Windows Server 2000. Over the last 20 years, a broad range of recommended practises have been defined for its maintenance and protection. In addition, the service has developed little in its most recent versions, as Microsoft allocated its development resources to cloud services such as Azure AD.

Information security features in Active Directory include:
• management and governance
• management of user credentials and groups
• central management of settings using Group Policy
• monitoring
• logs and alarms.

Defining thousands of Group Policy settings manually would be difficult. This is why Microsoft has released Security Baseline documents, which define these settings at specific information security levels. The most recent of these tools is called Security Compliance Toolkit (SCT)[26].

Requirements related to passwords are also controlled using the Group Policy feature. In Azure AD, a password must consist of 8–16 characters and, as a complexity requirement, it must include at least three of the following: uppercase letters, lowercase letters, numbers and special characters. In May 2019, the maximum length of passwords was increased to 256 characters. However, if the local AD is integrated with Azure AD, the on-premises password policies are applied instead. In other words, in the worst case, it is possible that Azure AD has one-character passwords for synchronised users.

Additionally, audit logs are usually defined centrally using the Group Policy feature. This document does not discuss any individual logs or their settings. With regard to phishing, auditing logs of login events must be ensured. Logs of individual computers and especially servers must be saved in a central location. This can be done using the Windows Event Forwarding feature of the Windows operating system[27]. Consolidated logs can be forwarded to SIEM systems, where events can be analysed more closely and alarms can be defined.

3.1.4 Modern authentication is a requirement for secure two-factor authentication

Modern authentication[28] is an umbrella term, covering combinations of different authentication and authorisation methods. For instance, two-factor authentication (2FA), or multi-factor authentication (MFA), requires the use of modern authentication.

Modern authentication is enabled in all Office 365 tenants generated after 1 July 2017. Configuration must be done individually for different services using PowerShell:
• Exchange Online[29]
• SharePoint Online[30]
• Skype for Business Online[31].

In hybrid environments, modern authentication must also be activated in the local Exchange[32] and Skype for Business[33] environment. Federated environments involve more deployment stages.

[22] https://docs.microsoft.com/en-us/office365/admin/setup/customize-sign-in-page?view=o365-worldwide
[23] https://aka.ms/aadpasswordprotectiondocs
[24] https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/
[25] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection

[26] https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10
[27] https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
[28] https://docs.microsoft.com/en-us/office365/enterprise/hybrid-modern-auth-overview#BKMK_WhatisModAuth
[29] https://docs.microsoft.com/en-us/Exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online
[30] https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditional-access-for-exo-and-spo
[31] https://social.technet.microsoft.com/wiki/contents/articles/34339.skype-for-business-online-enable-your-tenant-for-modern-authentication.aspx
[32] https://docs.microsoft.com/en-us/office365/enterprise/configure-exchange-server-for-hybrid-modern-authentication
[33] https://docs.microsoft.com/en-us/skypeforbusiness/manage/authentication/use-adal

3.1.5 Block legacy methods not supporting two-factor authentication

Conventional email protocols such as POP, IMAP, SMTP and ActiveSync do not support modern authentication. If two-factor authentication is used, the username and password combination can still be used through these protocols. The use of these protocols must be blocked, and the Office client software or other applications that support modern authentication must be used on computers and mobile devices.

The Exchange service plays the most important role in preventing phishing. The use of modern authentication may have been forced in federated environments using rules defined in AD FS[34]. In the autumn of 2018, it became possible to prevent basic authentication in the Exchange service using authentication policies that can be assigned even to individual users[35].

In Azure AD, it has been possible to prevent the use of applications that do not support modern authentication (including Exchange) since the summer of 2018[36] using conditional access rules. In the figure below, the "Client apps" condition has been defined to prevent the use of applications that do not support modern authentication.
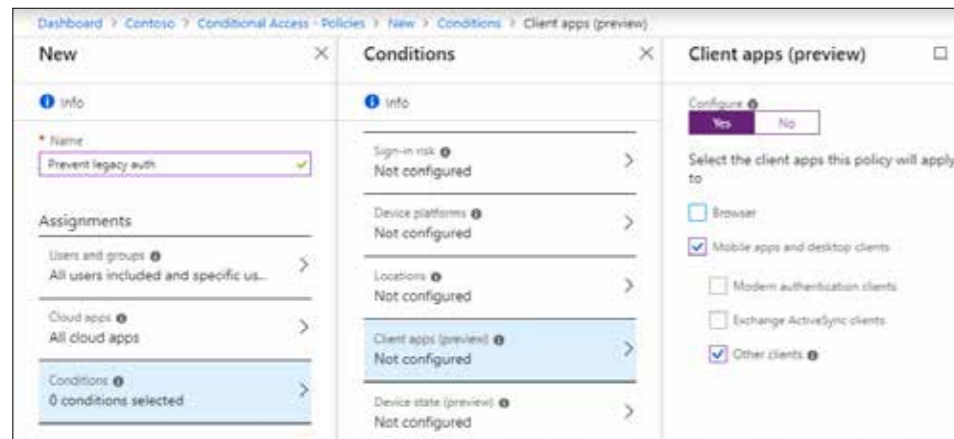
Options to enforce modern authentication are presented in the following table.

| Implementation method	Advantages	Challenges
AD FS rules	Operating system service. The service prevents the use of unsafe protocols and authentication from outside the internal network.	Only available in federated environments. More complicated rule definition (separate "programming language").
Settings at service level (Exchange Online)	Can be set for individual users.	If not a default policy, must be activated individually for each user.
Conditional access	Easy to implement.	Requires an Azure AD Premium subscription.

3.1.6 Modern authentication support in applications

Modern authentication requires support and possibly actions in the applications used.

All Office 365 services support modern authentication. When using services with the browser, modern authentication is the only available authentication method. However, other client software, such as email (Outlook) and instant messaging (Skype for Business),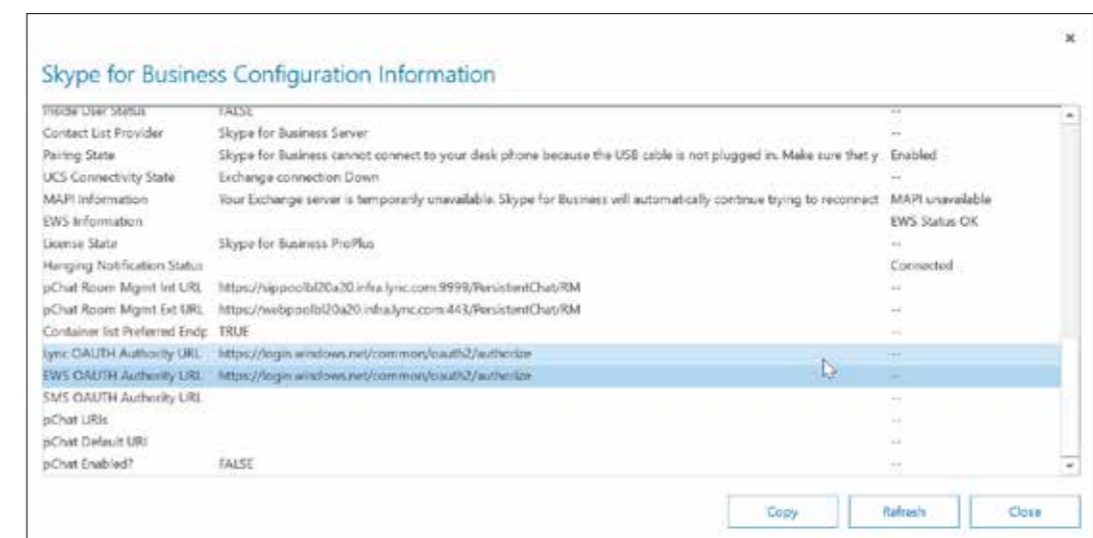 may require actions on workstations, depending on the Office version used. Office 2016 supports modern authentication by default. In Office 2013, it must be activated separately[37].

The use of modern authentication can also be checked on the workstation application. Outlook and Skype for Business are presented here. The user has clicked on the application icon in the system tray while holding the Ctrl key and selected Connection Status (Outlook) and Configuration Information (Skype for Business).
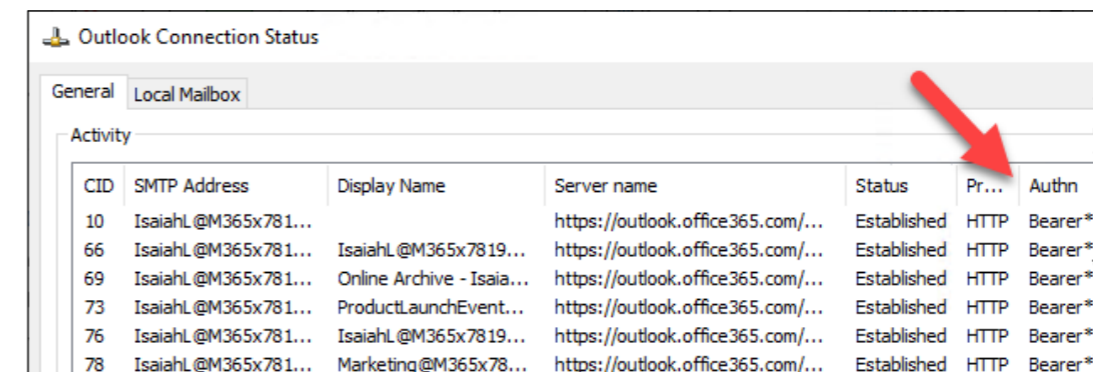
In Apple iOS, support for modern authentication was included in version 11. However, it has minor deficiencies that were fixed in version 12. Apple macOS 10.14 was the first version which included support for modern authentication. In Android, native email applications do not support modern authentication. This support is available in certain third-party client apps such as Nine, released by 9Folders[38]. Microsoft's client applications, such as Outlook for Android, support modern authentication.

[34] https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditional-access-for-exo-and-spo
[35] https://blogs.technet.microsoft.com/exchange/2018/10/17/disabling-basic-authentication-in-exchange-online-public-preview-now-available/
[36] https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Conditional-Access-support-for-blocking-legacy-auth-is/ba-p/245417
[37] https://docs.microsoft.com/en-us/office365/enterprise/modern-auth-for-office-2013-and-2016
[38] https://www.9folders.com/

3.1.7 Implement two-factor authentication

Ensure that you have implemented modern authentication as described above, so that there are no backdoors for two-factor authentication, i.e. it is truly secure.

Two-factor authentication can be enabled separately for each user or by using conditional access. Of these, the user-specific assignment became available first, and it can be activated without any Azure AD Premium licences. It is also possible to define that, after a successful authentication, no additional authentication is carried out in the following 1–60 days. However, this is not recommended. If a device is stolen, it could be used for access without any two-factor authentication.

Using Azure MFA, it is possible to define desired IPv4 address subnets in which two-factor authentication is skipped. If federated identity and AD FS are used, this can also be done using AD FS rules.

If a more complicated solution is needed for an on-premises environment, MFA Server[39] can be installed on the on-premises server. This also allows two-factor authentication to be activated in services other than those integrated with Azure AD. These services include Remote Desktop, local IIS web apps and applications that use AD FS for login.

Users need to define settings for two-factor authentication[40]. This can be done in the Access Panel portal https://myapps.microsoft.com or directly https://aka.ms/mfasetup. Designed to provide a smoother user experience, a converged site for self-service portal for passwords and MFA settings was being tested in February 2019 when this document was being written[41]. This site needs to be configured in tenant settings.

Users who have not yet registered 2FA/MFA with specific methods present a challenge to the process. A successful phisher may be able to register their own MFA method instead of the real user. As stated above,

Azure AD Identity Protection includes a forced registration feature. If Identity Protection is not available, the MFA status of users can be monitored using the MFA portal or PowerShell[42].

Two-factor authentication also presents additional steps for administrators using PowerShell. Depending on the service, the PowerShell module used may need to be replaced, or a connection with a cloud service may need to be established in a manner that differs from the previously used username and password combination.

3.1.8 Start using conditional access

Conditional access should be implemented by creating several policies. At first, this feature should be tested with a small group of users. Microsoft has released instructions for the use of conditional access[43].

Example policies suitable for testing and smaller environments are presented below:
1. Require MFA from administrators, apart from "break glass" administrators[44].
2. Require MFA when using unauthenticated devices.
3. Prevent legacy authentication for all users.
4. Prevent ActiveSync for all users.

Appendix 1 presents broader example policies suitable for a test environment. More detailed instructions are available for defining similar policies[45].

3.1.9 Secure on-premises AD authentication

Azure AD comes with versatile security features that Microsoft's large size enables it to offer. Similar resources may not be available in on-premises environments, and operating systems do not include advanced built-in features for detecting attacks.

Microsoft released Advanced Threat Analytics

(ATA)[46] in the summer of 2015. It helps to monitor traffic on on-premises AD domain controller servers to detect any abnormal behaviour of identities and any attempts to exploit many different vulnerabilities. Traffic monitoring can be carried out by means of port mirroring or by installing the ATA Lightweight Gateway app on specific domain controller servers. This feature is included in the EMS E3 licence.

Azure Advanced Threat Protection (Azure ATP)[47] is the cloud version of ATA, in which local ATA servers do not need to be installed. Instead, the Azure ATP Sensor app is installed on domain controller servers. This feature became available in March 2018 and is included in the EMS E5 licence.

3.1.10 Take care of users with administrator roles

It has been best practise that separate administrator credentials be set up in AD for management. However, these credentials continuously include all group memberships, which means these credentials are like hidden gems – to which attackers try to gain access.

This can effectively be prevented in Azure AD using the Privileged Identity Management feature. Microsoft recommends that there should only be two permanent Global administrators and no more than five in larger organisations. Conditional access and two-factor authentication should be disabled from these accounts (i.e. break-class accounts) so that they can log in, even if there are problems with services.

Microsoft Identity Manager (MIM) 2016 offers similar features in on-premises environments. This solution is called Privileged Access Management for Active Directory Domain Services[48]. Its deployment and maintenance require considerable resources.

Information security can be improved further by limiting administrative access to Privileged Access Workstations (PAW).

3.1.11 Challenges in security implementation

Federation in Azure AD has been implemented using standard WS-FED and SAML protocols. An information security vulnerability[49] has been discovered in federation implementation in Azure AD. It allows global administrators to log in as any organisational user without password, also allowing MFA to be bypassed. As Microsoft considers this vulnerability as a feature, it will probably not be fixed. Thus, the number of Global administrators must be minimised, and the actions of administrators related to this vulnerability must be audited.

Two-factor authentication also presents other challenges. In larger organisations especially, the number of IP subnetworks and their maintenance in MFA settings may be challenging. Country-specific restrictions can be bypassed using different VPN solutions. This means that two-factor authentication can be circumvented in real time, at least in theory.

[39] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-whichversion

[40] https://support.office.com/article/ace1d096-61e5-449b-a875-58eb3d74de14.aspx

[41] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-converged

[42] https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

[43] https://aka.ms/deploymentplans

[44] https://aka.ms/breakglass; 'break glass' is an analogy to an emergency button covered by glass, in other words, credentials used for exceptional situations only that can be used without MFA and conditional access

[45] https://bloggerz.cloud/2019/01/02/conditional-access-are-you-really-getting-the-most-out-of-it-part-2-of-2/

[46] https://docs.microsoft.com/en-us/advanced-threat-analytics/

[47] https://docs.microsoft.com/en-us/azure-advanced-threat-protection/

[48] https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

[49] https://ieeexplore.ieee.org/abstract/document/8456101

3.2 Securing email

3.2.1 Secure email routing

Exchange Online allows emails to be protected, for example, using connectors[50] between Exchange online and on-premise email server or email servers of trusted partners.

Email traffic between partners must always be encrypted using TLS, and the other party must be authenticated using certificates. It is recommended that the certificate includes a character set identified by the other party, such as the name of the company or the email domain. If the IP addresses of the other party's email servers are known, incoming mail can only be permitted from these addresses.

Permitted addresses defined by the sender can be identified from the SPF record using the following Windows command: nslookup -q=TXT partner.fi.
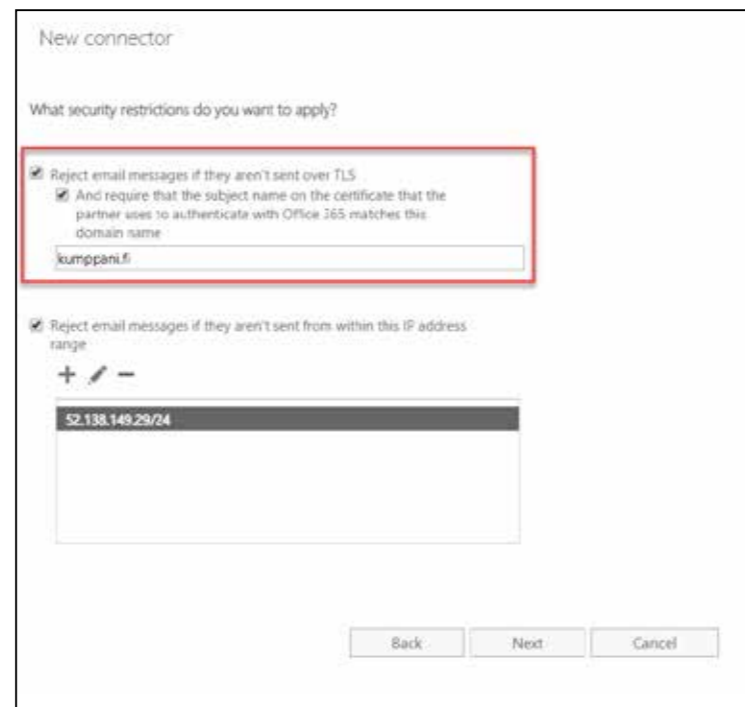
A phishing email may be sent from outside the organisation so that a fake address from the organisation has been defined as the sender. This route can be blocked using SPF. First, the SPF record must be set correctly in DNS. Next, "SPF Record: hard fail" must be activated in the spam settings of Exchange Online (Exchange admin center => protection => spam filter). This defines that emails sent in the organisation's name can only be received from the permitted sources listed in the SPF record.
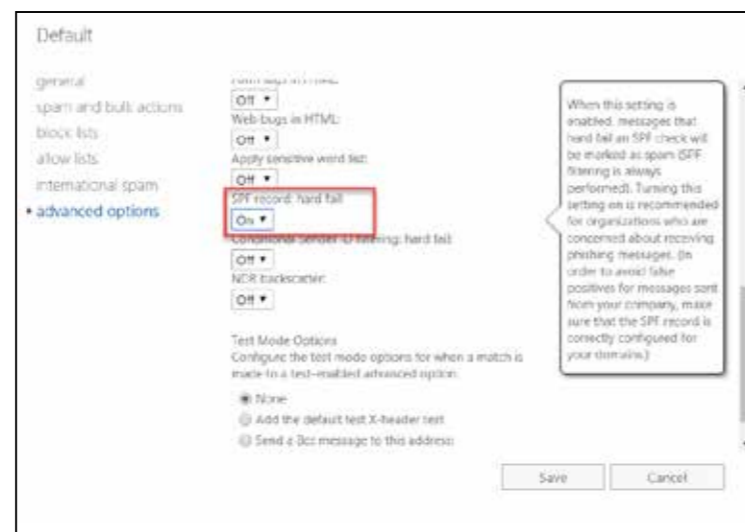
3.2.2 Securing users against malware and junk mail

Office 365 Advanced Threat Protection (Office 365 ATP)[51] protects users against malware, junk mail and phishing.

ATP Safe Attachments feature offers protection against zero-day attacks. Message attachments that pass checks of known malware and viruses are forwarded to a separate check environment. There, attachments are checked by means of machine learning to detect any unknown threats. If a file appears to have any malicious content, it will be deleted. Otherwise, the message and its attachment will be forwarded to the user's inbox.

ATP Safe Links is another useful feature in Office 365. It replaces any suspicious links with an error page indicating that the link may include malware or lead to a phishing page.

ATP Antiphishing checks whether incoming messages include phishing or impersonation attempts. It also uses different machine learning methods to analyse messages.

Office 365 ATP is included in Office 365 Enterprise E5, Office 365 Education A5 and Microsoft 365 Business.

Antiphishing is also available without ATP, but as a smaller version. Incoming messages are checked in the event of spoofing but not in impersonation attempts.

3.3 Logging and integration into SIEM systems

Different Office 365 services save user events in logs. The most important logs are those gathered by Azure AD and the Office 365 audit log. The Office 365 audit log must be activated separately[52], while other logs are enabled automatically, depending on the Azure AD version. The following table lists different logs and their data retention periods (which are very limited).

The audit log collects data about actions taken by administrators, such as the creation of new users and resetting passwords.

Sign-in log includes data about user logins. This is only available in Azure AD Premium subscriptions.

Office 365 audit log collects data about actions taken by administrators and users. It collects data from all services, including Azure AD audit and login activity logs. It has longer retention periods than other logs.

Delay of Azure AD logs, i.e. how quickly events appear in the logs, is approximately 15 minutes. In the Office 365 audit log, the delay is mainly 30 minutes, except in the case of Azure AD logs, which have a delay of 24 hours.

Log monitoring helps to identify phishing attempts when they occur. In practice, real-time monitoring requires the Azure AD Premium subscription, as the Office 365 audit log's delay is 24 hours.

It is recommended that the logs are transferred to an external system in which they can be stored lon-

Azure AD version and retention period (days)			
Log	Basic	Azure AD P1	Azure AD P2
Audit log	7	30	30
Login activity	-	30	30
Use	30	30	30
Risky users	7	30	30
Risky logins	7	30	30
Office 365 audit log	90	365	365

[50] https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/use-connectors-to-configure-mail-flow

[51] https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description
[52] https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

ger and analysed if necessary. Microsoft Azure offers such services.

Azure Monitor is a combination of monitoring, analysis and automated responses in cloud and on-premises environments. Audit and login activity logs can be transferred from Azure Monitor to Log Analytics for further analysis and visualisation. They can be stored in Azure (Storage Account) so that 1–365 days or an unlimited period can be set as the retention period. Storage costs must be taken into account especially in larger environments with a high number of login activities and, therefore, log events.

Logs can also be transferred to Azure Event Hub, from where they can be sent to the security information and event management (SIEM) systems of other manufacturers. For example, Sumologic[53], Splunk[54], IBM QRadar[55] and Micro Focus ArcSight[56] are SIEM systems that can be integrated with Azure.

The use of Azure Monitor services requires a separate Azure subscription, which is not included in Microsoft 365 or Office 365 subscriptions.

3.4 Monitoring

Office 365 and Azure both include various management portals which in turn include many different reports. Microsoft has realised the challenge presented by multiple portals, and it has started to integrate them. At the Ignite conference held in the autumn of 2018, new service management portals were demonstrated such as Microsoft 365 admin center https://admin.microsoft.com, which was still at the pre-version stage when this document was being written in February 2019.

PowerBI is a rapidly expanding analysis and reporting tool for different services. In February 2019, Microsoft released a method of using it for reporting alarms generated in different services . It can also be used to analyse login logs using the Azure Active Directory Power BI content pack[58].

3.5 Control and secure end user devices

Office 365 services are used on many different types of devices that can be owned by the user (bring your own device, BYOD) or the organisation.

Information security on devices is an integral part of system-wide information security. For example, if malware that monitors the user's actions is installed on a device, or its operating system is replaced by an unofficial version, the use of Office 365 services by all users on that specified device is at risk.

There are various options for the management of devices and their applications, such as:
- Office 365 Mobile Device Management[59]: smaller mobile device management (MDM) than in Intune, not including mobile application management (MAM), app distribution, profile management or PC and MacOS management
- Microsoft Intune (with MDM and MAM)
- Solutions of other MDM manufacturers, such as Citrix Endpoint Management (former Xen Mobile), MobileIron Unified Endpoint Management, IBM MaaS360 and VMware Workspace ONE (former AirWatch).

Of the solutions presented above, Microsoft's solutions integrate most tightly with Azure AD, and they allow devices to be registered in Azure AD. The compliance of devices with requirements can therefore be saved in device object settings. This data can, for example, be used in conditional access policies so that it can be required that devices on which specific services are used comply with requirements.

For decades, Windows workstations have been controlled by group policy settings defined in AD. Over the years, Microsoft's System Center Configuration Manager (SCCM) has become a widely used system for application management and inventory, particularly in larger environments.

However, Windows 10 and consumerisation are changing this. In recent years, Microsoft has developed the AutoPilot™ service, which is similar to Apple's Device Enrollment Program (DEP). With

autopilot, Windows 10 workstations can be adapted to meet the organisation's needs without conventional customised installation package. Workstation settings can be controlled using MDM solutions, such as Microsoft's Intune.

Windows 10 devices can currently be connected with Azure AD in following different ways:
- Azure AD Registered: devices owned by employees are registered in Azure AD and possibly in the organisation's MDM system
- Azure AD Joined: devices owned by the organisation are only connected with Azure AD
- Azure AD Hybrid Joined: devices are connected with both the on-premises AD and Azure AD. If a federated identity and AD FS are used, rules can be defined to limit the use of Office 365 on the organisation's devices only.

3.6 Provide users and administrators with proper training

User training is very important, as users are often the weakest links in information security. On the other hand, organisations of a thousand people can never achieve a situation where people make no mistakes when phishing attempts are made. However, if users have better skills and a higher level of awareness, attacks have lower chance to succeed.

Each Office 365 user should know how to safeguard their password and identify fake messages, and what to do if they are targeted by a phishing attempt, or if such an attempt has succeeded.

Training can, for example, include the following:
- What makes a good password – the longer the better.
- Attackers usually approach users via email, but they can also use calls and text messages.
- If the linguistic content of a message is poor, it is probably a fake message.
- If the visible part of the hyperlink differs from the link in the background, the message is probably fake.
- If the target URL of the hyperlink is numerical, the message is probably fake.
- If the target URL of the hyperlink resembles a respectable company, the message is probably fake. Example: not www.gigantti.fi but www.gigamtti.fi

- If the message asks the user to act immediately and includes a threat of loss of income, it may be a scam.
- If the linguistic content seems artificial, the message is probably fake.
- A message may appear real because it was sent from the email address of a director or a colleague. However, it was sent by an attacker, meaning that the request presented in the message is a scam.
- How can a real login screen be distinguished from a fake one?
- If you receive a scam message and you do not fall for it, it must be deleted. It does not need to be reported separately.
- If you accidentally enter your password on a page that you know or suspect is a phishing page, immediately report the situation following your organisation's instructions.

Considering the importance, and also narrow scope of phishing, it would be useful to test or otherwise identify the level of knowledge of each user.

The content of training must be adapted when technologies and situations change.

In addition to training, users can also be tested, which is also part of their training. An organisation's data management sends phishing messages to users. If users click on the link, they will be forwarded to a page which offers information about phishing.

Office 365 includes Attack Simulator, a feature for simulating attacks. Similar simulations and training can also be purchased as a service from third parties.

The skills of administrators and their understanding of the most recent threats must also be ensured. Microsoft has been changing its certification program since the autumn of 2018. Securing the Microsoft 365 environment and developing the level of information security are covered, for example, in the following new role-based certifications and related training:
- Microsoft 365 Certified: Security Administrator Associate[60]
- Microsoft 365 Certified: Enterprise Administrator Expert[61].

[53] https://help.sumologic.com/07Sumo-Logic-Apps/04Microsoft-and-Azure/Azure_Active_Directory/Install_the_Azure_Active_Directory_App_and_View_the_Dashboards
[54] https://splunkbase.splunk.com/app/3534/
[55] https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/t_dsm_guide_microsoft_azure_enable_event_hubs.html
[56] https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-for-Microsoft-Azure-Monitor-Event-Hub/ta-p/1671292
[57] https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Gain-rich-insights-with-the-new-Microsoft-Graph-Security-Power/ba-p/334467
[58] https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-power-bi-content-pack
[56] https://support.office.com/en-us/article/Frequently-asked-questions-about-Mobile-Device-Management-for-Office-365-3871f99c-c9db-4a23-86f9-902c1b02f58d

3.7 Use checklists

Due to the general nature of phishing attempts, there are many checklists available to mitigate them. Microsoft has released a series of blog articles https://blogs.technet.microsoft.com/cloudready/2018/07/31/introduction-email-phishing-protection-guide-enhancing-your-organizations-security-posture/. Not all its detailed articles are fully up to date, but their instructions can be applied with the data sources listed in this document.

The description of the deployment stages for the Microsoft 365 identity infrastructure https://docs.microsoft.com/en-us/microsoft-365/enterprise/identity-infrastructure presents how a hybrid identity and its most important features can be implemented.

The Secure Score portals described above in this document include lists of features, many of which help to reduce the success of phishing.

3.8 Password-less sign-in

As stated many times in this document, the main goal of phishing is to steal user credentials (i.e. usernames and passwords) and to misuse them in one way or another. Users can also be authenticated without any passwords.

For example, in its services, Microsoft has presented Windows 10 Hello for Business[62], in which users are authenticated by entering a PIN code or by biometric means.

Using AD FS, Azure MFA can be defined as the primary authentication method in federated environments[63]. The minimum requirement is Windows Server 2016 AD FS.

Users can also log in without any password using the Microsoft Authenticator mobile app[64]. This provides users with a number sequence, and users need to tap a corresponding part of their phone screen to approve the login.

Some sectors and organisations also use smart cards. In this case, users may not even know their password, and they log in using their smart card and its PIN code.

[60] https://www.microsoft.com/en-us/learning/m365-security-administrator.aspx

[61] https://www.microsoft.com/en-us/learning/m365-enterprise-administrator.aspx

[62] https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification

[63] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa

[64] https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-phone-sign-in

Phishing threats and their mitigation

Threat	SaaS — Office 365 version			Authentication and authorisation (identity) — AAD version		
	Business	E3	E5	Basic ja Office 365	AAD P1	AAD P2
Phishing message to a user						
Anti-spoofing, fake messages	TLS used with certain partners	‹	‹			
Ensured security of links	›	›	Safe links			
Unauthorised access to identification data						
Cracking passwords (brute force)				Protecting passwords / Extranet lockout if federated authentication is used	‹	‹
Easily distinguished login pages				Customised login pages	‹	‹
Insufficient username and password pair				User-specific two-factor authentication (MFA for Office 365) / If federated authentication is used, AD FS conditional access rules	Two-factor authentication (Azure MFA), conditional access	+ Identity Protection, forced MFA registration ‹
MFA bypass						
Use of legacy protocols	Basic authentication prevented in Exchange	‹	‹	Basic authentication prevented in Exchange (in Office 365, not as an AAD function), or ›	Forced modern authentication using conditional access	‹
Real-time MFA phishing (e.g. phishing confirmation text messages)						
Data leak – email						
Prevented mail forwarding rules	Automatic forwarding prevented in default remote domain configurations, transport rules	‹ + Data Loss Prevention (DLP)	‹			
Prevented inbox rules						
Outgoing junk mail	Throttling transmitted mail / Connector settings, e.g. authentication	‹	‹			
Data leak from other services						
Single sign-on used to log in to other systems				Monitoring - sign-ins	‹	
Unauthorised sharing of documents from SaaS	›	›	Office 365 Cloud App Security / Microsoft Cloud App Security available with the EMS licence			
Other misuse of credentials						
Lateral movement				›	ATA	Azure ATP
Making use of protocol weaknesses				›	ATA	Azure ATP
Misuse of administrator credentials						Privileged Identity Management

Explanations:
› Can be implemented by acquiring a more expensive licence from the right-hand bar
‹ Can be implemented as defined on the left
▮ Threat irrelevant in this context or protection impossible

Observations and forensics

Threat	SaaS — Office 365 version*			Authentication and authorisation (identity) — AAD version		
	Business	E3	E5	Basic ja Office 365	AAD P1	AAD P2
Logging						
Cracking passwords (brute force or spray attack) – on-premises				Monitoring event logs	‹	‹
Cracking passwords (brute force or spray attack) – AAD				Monitoring login activity logs	‹	‹
Attempts to misuse credentials – on-premises				On-premises: monitoring event logs	‹	‹
Attempts to misuse credentials – AAD				Monitoring login activity logs	‹	‹
Investigating any messages read						
Investigating searches made in inbox content	Investigation of logs	‹	‹			
Identifying mail forwarding rules	Investigation of logs / Investigating inbox settings	‹	‹			
Identifying inbox rules	Investigation of logs / Investigating inbox settings	‹	‹			
Identifying emails sent from a hacked account	Investigation of logs	‹	‹			
Investigating searches made in inbox content				› Sign-in logs		‹
Preventive monitoring						
Identifying the misuse of credentials				›	Azure Active Directory risk events	‹
Identifying successful phishing				›	Azure Active Directory risk events	‹

Explanations:
› Can be implemented by acquiring a more expensive licence from the right-hand bar
‹ Can be implemented as defined on the left
▮ Threat irrelevant in this context or protection impossible

The table summarises threats and attacks related to Office 365 phishing and data breaches, as well as protection and observation methods available at licence levels commonly used in Finland. The table is not an exhaustive service description, but it offers help in identifying available means within the scope of current licences.

4 What to do in the event of an attack

Each organisation's information security instruction should include internal operating instructions, i.e. a description of their security incident process. The instructions presented in this document should be added to organisation-specific instructions where applicable.

A brief checklist of what to do in the event of an attack is given below:

1. Identify the targeted victims and accounts, and prevent any further damage (take over the attacked user accounts, lock the attackers out and take direct action to mitigate any damage).
2. Communicate the situation internally to minimise any further damage.
3. Prepare an initial assessment of the attack and the scope of damage as far as possible.
4. Communicate the situation externally to prevent the damage from spreading (preliminary contact with the authorities).
5. Investigate the chain of events from logs. What happened and when? Who did what?
6. Clean any contaminated files and data. Archive log files for later use.
7. Report any new information to the authorities.
8. Ensure long-term protection against similar attacks.

4.1 Blocking logged-in attacker

If it is known or suspected that specific credentials have fallen into the wrong hands and may be used by an attacker, the access of these credentials to different Office 365 services can be blocked. However, these services may cache older data to make regular use smoother. This means that attackers may be able to use these credentials even after passwords have been changed. As a result, it is necessary to sign out currently used connections.

This can be done in the Office 365 management portal. First, open properties of the hacked user and consequently OneDrive settings. These include the functionality shown in the adjacent image.

Click on the Initiate link to prevent any connections associated with the specific credentials for the next 15 minutes on all devices. To prevent the attacker immediately signing in again, new logins must also be blocked. In the "Sign-in status" section in user data, you block user as shown in the adjacent image.
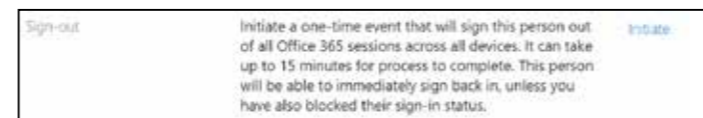
Once the changes have been saved, a pop-in window will request you to change the password, and you should do so as quickly as possible.

If the targeted user was synchronised from the local AD directory and the password was changed there, its transfer to the Azure AD cloud can be checked by using the Get-MsolUser command in PowerShell and checking the LastDir-SyncTime and LastPasswordChangeTimestamp dates from the results.

In addition, the following two PowerShell commands can be used to sign out connections:

- Revoke-SPOUserSession is a SharePoint Online command which signs out the targeted user's SharePoint connections.
- Revoke-AzureADUserAllRefreshToken is an Azure AD command which signs out the targeted user's connections with all applications that use Azure AD.

Finally, check whether the targeted user's inbox includes any delegates. If the user's password has fallen into wrong hands, it can also be used to gain access to the inbox.

4.2 Prevention/forensics/investigation

The first step after an attack is to raise the level of information security regarding the entire tenant by forcing two-factor authentication for all users. If Azure AD Premium of AD FS is used, any use from outside the organisation and unauthenticated devices should also be prevented. These actions effectively stop an attack in progress while allowing the organisation to continue its operations.

Next, the victims of the attack need to be identified. This can be done using the following data sources and methods.

Once the victims have been identified, sending email from their email accounts to recipients must be prevented using the rules. This prevents new phishing messages and junk mail spreading and reaching new victims. If Exchange Plan 2 is used, the inboxes of the victims should immediately be placed in legal hold to ensure that no evidence is lost.

Data source/method	What is investigated?
Audit log	Are there any irregular events, such as created domains or changes in their authentication methods? Have any changes been made to logging?
Login activity	Are there any irregular login dates and locations?
Office 365 audit log	Have email rules been created? Attackers may add a mail forwarding rule to their inbox in order to monitor specific messages.

After the security has been hardened, all available logs need to be collected to maintain and analyse evidence.

National Bureau of Investigation has pointed out that difficulties in obtaining information is a challenge when investigating Office 365 data breaches. It is therefore vital to save log data in Office 365 service.

Office 365 audit logs help to identify any unauthorised logins and the IP addresses of the attackers, and to reveal at least some of the unauthorised actions taken in the system. Without any log data, it is nearly impossible to identify compromised data and prove that a data breach has taken place.

Where prevention is concerned, it is recommended that customers check whether they are saving log data, where this log data is available and how far back the logs go.

In the event of a data breach, we recommend reporting the offence to the police (or sending a Net tip) as quickly as possible so that log data is available over a sufficient period.

4.3 Contacting NCSC-FI

NCSC-FI is interested in receiving information about all phishing messages and data breaches involving Office 365. We use this information to build nationwide situation awareness and, for example, to send disconnection requests regarding phishing sites.

You can report this information to NCSC-FI via email cert@traficom.fi or by using the information security breach form on the website: https://www.kyberturvallisuuskeskus.fi/en/report

4.4 Contacting the police

Hacking user accounts and using them without proper authorisation can be regarded as a data breach. They may also be regarded as other offences. This will be specified during investigations by the police. An offence can be reported by calling or visiting the local police department or online at https://www.poliisi.fi/crimes/reporting_an_offence_online

If phishing was not successful, or if the organisation does not want to report the offence for some reason, a Net tip should still be sent to the police. All information about the chain of events and attackers can help to investigate other attacks or to build an overview of larger criminal activities. A Net tip can be sent at https://www.poliisi.fi/nettip

4.5 Notifying the Office of the Data Protection Ombudsman

Nearly all Office 365 data breaches targeting organisations also concern personal data.

Data breaches targeting personal data must be reported to the Office of the Data Protection Ombudsman and to the persons targeted by the breach if the breach presents a high risk to data subjects.

After reporting data breaches to the Office of the Data Protection Ombudsman, data controllers can obtain information and guidance regarding the protection of personal data. This notification also helps the managers of the organisation to build situation awareness. If required, the Data Protection Ombudsman can order the organisation to fulfil its obligations set out in the EU General Data Protection Regulation (GDPR).

Following the notification, the process proceeds as follows with regard to Office 365 data breaches:
1. It is ensured that the attack is no longer active.
2. The scope of the attack regarding personal data is identified.
3. The number and quality of leaked personal data are identified.
4. The extent to which the breach presents a high risk to data subjects is assessed.
5. If required, the Data Protection Ombudsman can order the organisation to fulfil its obligations set out in the EU General Data Protection Regulation.
6. Documentation and additional instructions as necessary. Normally the following additional information is requested regarding Office 365 attacks. This information also acts as documentation related to the data breach. Further log data will also be requested as necessary.

Additional information about Office 365 data breaches:
1. Is the environment Office 365 or OWA?
2. Has it been verified that no unauthorised forwarding rules have been added to accounts?
3. If they have, what are the addresses defined in these rules?
4. Has it been verified that no unauthorised entry in these accounts has taken place during this time (e.g. Azure AD sign-in log)?
5. If any unauthorised entry has taken place, has it been verified that no emails have been downloaded (e.g. Office 365 Exchange logs)?
6. Were any OneDrive or SharePoint services used in the account?
7. Did the emails or OneDrive or SharePoint services include any personal data?
8. If they did, how many people did this personal data concern and what personal data categories were represented (e.g. name, personal identity code, email address, regular address)?
9. Has implementing MFA been considered?
10. Regarding leaked credentials, the Azure AD Sign-in log over the attack period must be sent to the Office of the Data Protection Ombudsman as a CSV file.

4.6 Financial administration controls

Hacked accounts have been used, for example, to create and/or send fake invoices. The targeted company must identify this threat in their invoicing processes, and when adding and editing account details.

NCSC-FI has received information about several cases where, after hacking email accounts, attackers intervened in email messages sent between organisations using the aforementioned forwarding rules and mail archiving, or edited existing invoices and account details. As a result, a valid invoice may have been sent to a customer or partner but, as attackers have edited invoice or account details, funds are sent to an incorrect bank account. Concerning fake invoices, this problem applies particularly to PDF invoices. No attacks have been targeted at electronic invoices thus far.

Organisations therefore need to internally define how invoice details are checked, how they send their invoices to their customers and how they verify any changes in the account details of their customers and partners.

4.7 Communication with stakeholders

As there is nothing out of the ordinary about being targeted by data breaches and misuse, organisations should plan communication templates and policies for different scenarios. In certain cases, a particular case may attract media attention and be made public. It is therefore useful to prepare a plan for these situations before anything happens.

If junk mail or phishing messages have been sent from the targeted user's email account, they will probably accumulate notifications and comments from recipients and their organisations. It is also possible that these will create victims in other organisations. It is therefore recommended to communicate proactively after a breach has been identified.

Special attention should be paid to internal communication. In very many cases, malicious messages have been sent from the account of the first victim to other members of the same organisation, so that the attacker captures a larger number of user accounts from a single organisation. The situation should therefore be communicated internally as quickly as possible and at a low threshold to minimise damage.

For further information, please contact:

tietosuoja(at)om.fi
Personal data breaches:
https://tietosuoja.fi/en/personal-data-breaches
Data breach notification:
https://tietosuoja.fi/en/data-breach-notification

Appendice

Appendix 1. Example of conditional access policies
The example includes two groups: sg_CA Excluded Cloud and sg_CA Excluded On-prem, whose members include the usernames and service IDs excluded from conditional access.

Name	Users and Groups		Assignments		Access controls	
	Include	Exclude	Device Platforms	Client Apps	Block access	Grant access
Allow modern authn from AADHJ or compliant devices - Clients	All Employees	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require device to be marked as compliant OR Require Hybrid AD joined device
Allow modern authn from AADHJ or compliant devices - Browser	All Employees	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require device to be marked as compliant OR Require Hybrid AD joined device
Require MFA for admins - Clients	Admin groups	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for admins - Browser	Admin groups	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require multi-factor authentication
Require MFA for Guests - Clients	All guest users	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for Guests - Browser	All guest users	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require multi-factor authentication
Require MFA for All other Users - Clients	All users	sg_CA Excluded Cloud sg_CA Excluded On-prem All Employees Admin groups All guest user	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for All other Users - Browser	All users	sg_CA Excluded Cloud sg_CA Excluded On-prem All Employees Admin groups All guest users	Android iOS Windows macOS	Browser		Require multi-factor authentication
Block ActiveSync	Cloud apps > Office 365 Exchange Online			Mobile apps and desktop cllients Exchange ActiveSync clients > Apply policy to supported platforms	Block	
Block legacy authn				Mobile apps and desktop clients > Other clients	Block	