Microsoft 365

Microsoft 365 Academy: Trailer

Michele Sensalari MCT Trainer michele@sensalari.com @ilsensa7



Michele Sensalari

- Senior Consultant Speaker Trainer
- Dipendente 50% su tecnologie Microsoft al Dipartimento di Informatica – Università degli Studi di Milano
- Freelance 50/70% (e si anche il we..)
- Docente, speaker, responsabile conferenze Overnet Education
- MCT, MCSE, MCSA. MCITP
- Contatti:
 - michele@sensalari.com
 - michele.sensalari@overneteducation.it
 - Twitter: @ilsensa7
 - Linkedin

WPC2018

Menù

Information Protection

Bitlocker

MAM / MDM

Microsoft Information Protection

Windows Information Protection

Azure Information Protection

Office 365 ATP

Information Protection



Sensitive data is at risk

80% of employees use non-approved SaaS apps at work

88 %

of organizations no longer have confidence to detect and prevent loss of sensitive data

58% Have accidentally sent sensitive information to the wrong person

85% of enterprise organizations keep sensitive information in the cloud



YOUR INFORMATION PROTECTION NEEDS

DEVICE	DATA	LEAK	SHARING
PROTECTION	SEPARATION	PROTECTION	PROTECTION
Protect system and data when device is lost or stolen	Containment Data separation	Prevent unauthorized users and apps from accessing and leaking data	Protect data when shared with others, or shared outside of organizational devices and control

YOUR INFORMATION PROTECTION NEEDS

DEVICE	DATA	LEAK	SHARING
PROTECTION	SEPARATION	PROTECTION	PROTECTION
BitLocker	Windows Informatic (MAM)	Azure Informa Office 365 n Protection	tion Protection

Bitlocker

Bitlocker Management



Microsoft Intune Bitlocker Management

Microsoft Azure		₽ Search resou	irces, services, and docs	
«	Home > Microsoft Intune > Device configuration	Profiles > Create profile > Endpoint protectio	n > Windows Encryption	
+ Create a resource	Create profile \times	Endpoint protection	X Windows Encryption Windows 10 and later	_ ×
Create a resource Create a resource Create a resource Create a resource Comparison C	Create profile × • Name Device Encryption Compliance Policy Description Description Device Encryption Compliance Policy • • Platform • Windows 10 and later • • Profile type • Endpoint protection • Settings > Onscope(s) selected >	Enclopoint Percent protection Windows 10 and later Select a category to configure settings. 10 settings available 10 settings available Windows Defender Application Gu 10 settings available Windows Defender Firewall 2 40 settings available 2 Windows Defender SmartScreen 2 2 settings available 2 Windows Defender Exploit Guard 2 2 settings available 2 Windows Defender Application Co 2 2 settings available 2 Windows Defender Application Co 2 2 settings available 2 Windows Defender Application Co 2 2 settings available 2 Windows Defender Security Center 1 1 setting available 2 Windows Defender Security Center 2 17 settings available 2 Local device security options 46 settings available Xbox services 5 5 settings available 2	Windows Electyption Windows 10 and later BitLocker OS drive settings ① Additional authentication at startup ① BitLocker with non-compatible TPM chip ① Compatible TPM startup ① Compatible TPM startup ② Compatible TPM startup Artup ② Compatible TPM startup Artup ② Compatible TPM startup key ③ Compatible TPM startup key ④ Compatible TPM startup key ● User creation of recovery agent ● User creation of recovery password ● User creation of recovery key ● Recovery options in the BitLocker setup wizard Save BitLocker recovery information to Azure Active Directory ● BitLocker recovery I	Require Not configured Block Not configured Block Not configured Require TPM V Require startup PIN with TV Allow startup key with TPM V Allow startup key and PINV Enable Not configured 6 V Enable Not configured Block Not configured Allow 256-bit recovery paV Allow 256-bit recovery key Block Not configured Enable Not configured Block Not configured Block Not configured Enable Not configured
			Store recovery information in azure Active Directory before enabling BitLocker o Pre-boot recovery message and URL o Pre-boot recovery message o	Require Not configured Enable Not configured Use default recovery mess.
	Create	OK	OK	1.555 SUBULINATION (1997)

Microsoft Intune BitLocker management platform is available today, and includes features such as compliance reporting, encryption configuration, with key retrieval and rotation on the roadmap. In the coming months, we expect Microsoft cloudbased BitLocker management to meet and exceed the MBAM capabilities you are familiar with.

New Feature Intune Bitlocker coming in 2019

Key recovery auditing

Get reports on who accessed recovery key information in Azure AD.

• Key recovery

Enables you or another admin to recover keys in the Microsoft Intune console. You may enable user self-service key recovery using the Company Portal app, available across device platforms such as web, iOS, Android, Windows, and MacOS.

• Key management

Enable single-use recovery keys on Windows devices by ensuring keys are rolled onaccess (by client) or on-demand (by Intune remote actions).

• Migrating from MBAM to cloud management

For our current MBAM customers that need to migrate to modern BitLocker management, we are integrating that migration directly into the key rotation feature

Microsoft Intune: MAM vs MDM



Microsoft Intune

The simplest way to manage all Microsoft 365 endpoints



Protect Office 365 data, even on unmanaged devices

Employees expect access to the best tools, wherever they are—even on their own devices. IT needs confidence that critical data is secure. Intune delivers both.

local storage

Identity-driven protection



Can I protect app data on an unknown device?



Introduction to Intune App Protection Policies (APP)



Familiar Office experience

- Seamless "enrollment" into app management
- Use for personal and corporate accounts

Comprehensive protection

- App encryption at rest
- App access control PIN or credentials
- Save as/copy/paste restrictions
- App-level selective wipe

MDM mgmt. by Intune or third-party is optional

Might be a good solution for these scenarios:

- BYOD when MDM is not required
- Extending app access to vendors and partners
- Already have an existing MDM solution

When should I require a device to be fully MDM managed?

- 1. Corporate vs. BYOD
- 2. What do users need to access?
- 3. Are there additional security requirements; certificates, S/MIME?

How should I protect data on a managed device?

- 1. Enrollment Restrictions
- 2. Windows Security Baseline Settings
- 3. Windows Hello
- 4. Encryption
- 5. Mobile Threat Defense

Microsoft Information Protection

Microsoft Information Protection solutions help you protect sensitive data throughout its lifecycle – inside and outside the organization



MICROSOFT'S INFORMATION PROTECTION SOLUTIONS



Protect files in libraries and lists

Microsoft Information Protection Protect your sensitive data – wherever it lives or travels



Devices

Apps

Cloud services

On-premises

Common use cases

Discover and understand the sensitive data across your environment

Accelerate your journey to the cloud by classifying, labeling and protecting data on-premises

Get control of data sprawl in the cloud by classifying, labeling and protecting files in 3rd-party cloud services

Implement an information protection strategy to meet compliance obligations

Windows Information Protection

WINDOWS INFORMATION PROTECTION

Integrated protection against accidental data leaks

8 Protects data at rest locally and on removable storage. Common experience across all Windows 10 devices with copy and paste protection. Corporate vs personal data identifiable wherever it rests on the device and can be Since Windows 10 Version 1607 wiped. **Prevents unauthorized apps** from accessing business data and users from leaking data Seamless integration into the platform, No mode via copy and paste protection. switching and use any app.

WIP Overview



- Windows Information Protection is an extension to the Windows 10 operating system
- Windows Information Protection (WIP) helps protect against additional areas of potential data leakage without interfering with the employee experience.
- WIP uses encryption to protect sensitive (work) content. By encryption it can disallow content to be copy/pasted into other documents. It also allows document to be blocked from sharing using non-protected apps (like e-mail) or storage on non-protected locations (like an USB drive)
- WIP differentiates between corporate and personal data and apps that can exist side by side on the same device
- There are two major components to WIP. There's the application which are allowed to access protected content and there's the location where this content is stored.
- Based on the settings of the policy, users can change the ownership from work to personal and visa versa (less restrictive). Or this ownership is applied automatically (more restrictive). WIP uses a set of content locations (fileshare, cloud storage, and more) to determine if the content is either personal or work related.
- WIP settings are delivered through policies to user devices, which need an MDM or MAM solution that supports WIP

Planning for WIP



- Implementing WIP requires the following prerequisites:
 - Windows 10 version 1607 (Anniversary Edition) or later
 - A MDM or MAM solution that supports the "EnterpriseDataProtection" configuration service provider (CSP) such as Microsoft Intune
 - Windows Client must be enrolled in MDM or registered for MAM
- Once you've satisfied your prerequisites, you should plan for the following issues related to your WIP implementation:
 - Determine which Policy protection mode to use: WIP has three simple policy enforcement modes. It lets you choose how and whether the user experience in the clipboard, save dialog, and similar data-sharing cases have options (overrides) to move work content to non-work context. You can decide to *Hide Overrides*, *Allow Overrides* for your users, or even deploy in *Silent mode* just for auditing. *Silent mode* does not restrict unmanaged apps from opening work data the way *Hide Overrides* and *Allow Overrides* do
 - Configure your intelligent network boundaries

Implementing WIP

- You can implement WIP by creating WIP policies in Microsoft Intune
- You can select a deployment for MDM (Windows 10 device is enrolled) and for MAM (Windows 10 device is not enrolled)
- To add a new WIP policy in the Azure Portal:
 - 1. Go to the Azure Portal
 - 2. Select All Services, type Intune and click it from the Service tab
 - 3. Open the Mobile apps from Manage
 - 4. Open the App protection policies from Manage
 - 5. Click Add a policy on the top to open the next tab



Business/Personal One experience Data is isolated Data is encrypted at rest Organization holds keys MDM / MAM managed Block/audit data exchange APIs for ISVs Office and OneDrive



Enlightened Applications



Unenlightened Applications – How to manage

- Option 1: Use Allow policy
 - Caution: Auto-encrypts all files touched
 - Intended for Line of Business (LOB) apps
 - Can include in policy for fully managed devices
- Option 2: Use Exempt policy
 - WIP rules don't apply to the app
 - Access work without impacting personal data
- Option 3: Enlighten the app
 - See: <u>http://aka.ms/wip-dev-guide</u>

Working with WIP in Windows Desktop

• The terms "Enlightened" and "Non-Enlightened" (or Unenlightened) describe applications with full support of separation between corporate and personal data and applications that can only recognize all their data as corporate work data

	A least Dick (C)	· Information Destaction d	10000		Carach Inform		0
← → *	T cocal Disk (C:)	> information Protection d	iemo	V 0	Search Inform	mation Protectio	þ
Organize 🕶	New folder					822 •	0
Name	^	File ownership	Date modified	Ty	pe	Size	
		No items mate	ch your search				
			,				
File	name 🔒 🔻 SaveThisF	ile.b.t					
File Save a	name 🔁 🔻 SaveThisf	ile.b.t microsoft.com)					
File Save a	name 🔁 🔻 SaveThisf is tipe: 📾 Work (corp.i Personal	ile.t.t nicrosoft.com)					~ ~



Azure Information Protection

The evolution of Information Protection



Planning AIP Solution

For AIP deployment, organizations must consider the following planning and configuration steps:

- 1. Prepare the Tenant for Azure Information Protection
- 2. Customize labels and policies
- 3. Deployment of Azure Information Protection client
- 4. Configure Rights Management and participating services
- 5. Rolling out AIP to the end users

AIP Labels Overview

- Labels contain different settings on how to mark and optionally protect documents, files, and emails that are sent to your end users
- Sub-labels can add additional settings to a label
- Before customizing labels, you must create your classification strategy
- Azure Information
 Protection provides a set of
 Default labels and policies
 that are created when you
 activate AIP for your tenant

Search (Ctrl+/)] « ■	olumns				
NERAL	LAE	EL DISPLAY NAME	POLICY	MARKING	PROTECTION	
ै Quick start		Personal	Global			
SSIFICATIONS		Public	Global			
Labels		General	Global			
Policies	•I	Confidential	Global			
NAGE		All Employees	Global	~	~	
Languages	-	Anyone (not protected)	Global	~		
Protection activation	2	Recipients Only	Global	~	~	
·		Highly Confidential	Global			
		All Employees	Global	~	~	
		Anyone (not protected)	Global	~		
		Recipients Only	Global	~	~	
	•	Protection templates				

Classification and labeling



0	It is recommended to label this file as Confidential as it contains credit cards	Change now
0	Sensitivity: 📕 General 💉	

Automatic classification

Policies can be set by IT Admins for automatically applying classification and protection to data.

Recommended classification

Based on the content you're working on, you can be prompted with suggested classification.

Manual reclassification

You can override a classification and optionally be required to provide a justification.

User-specified classification

Users can choose to apply a sensitivity label to the email or file they are working on with a single click.

Working with AIP Labels

- You can see your configured labels and sub-labels when opening suported Office application on a client that has the Azure Information Protection client installed
- You can use Azure Portal to create additional labels (and sub-labels) with special settings for your users



Configuring AIP Policies

- A policy is an additional set of rules that are used to group labels to be available for users or groups
- All predefined labels and sub-labels in Office 365 are configured in the default policy named "Global"
- You cannot scope Global policy to any specific users or groups
- The following rules apply when creating new policies:
 - Custom labels can be added to only one policy
 - To add a sub-label, its parent label must be in the same policy or in the global policy
- The Azure Information Protection client checks for any changes whenever a supported Office application starts

tome > Azure Information Protection - Policies > Policy: Global Policy: Global ensalarLab - Azure Information Protection Coloringure administrative name, description and scope for this policy Policy name Global Policy anne Global Policy or all users in the tenant All EL DISPLAY NAME POLICY MARKING PROTECTION Personal Global Flighly Confidential Global
Policy: Global
Installan Lab - Adure Information Protection Columns Save Discard Di
■ Columns ■ Save ▲ Discard ■ Delete ▲ Export onfigure administrative name, description and scope for this policy Policy name Global
Policy name Global Object of the spolicy of the spolicy. Groups must be email-enabled. Policy MARKING Policy Global Policy Globa
Policy name Global olicy description Default policy for all users in the tenant all Select which users or groups get this policy. Groups must be email-enabled. POLICY MARKING PROTECTION Image: Personal Global POLICY MARKING PROTECTION Image: Personal Global Clobal
Global
Default policy description Default policy for all users in the tenant Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups get thi
Default policy for all users in the tenant all Select which users or groups get this policy. Groups must be email-enabled. LABEL DISPLAY NAME Personal Global Public Global Global Global Global Highly Confidential Global Add or remove labels Configure settings to display and apply on Information Protection end users Title
Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users of Global Image: Select which users or groups get this policy. Select which users of Global Image: Select which users or groups get this policy. Select which users of Global Image: Select which users or groups get this policy. Groups must be email-enabled. Image: Select which users of Global Image: Select which users or groups get this policy. Select which users of Global Image: Select which users or groups get this policy. Select which users of Global Image: Select which users or groups get this policy. Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image: Select which users of Global Image:
Select which users or groups get this policy. Groups must be email-enabled. LABEL DISPLAY NAME POLICY MARKING PROTECTION Personal Global Public Global Global Global Confidential Global Global Add or remove labels onfigure settings to display and apply on Information Protection end users Title
LABEL DISPLAY NAME POLICY MARKING PROTECTION Image: Personal Global Image: Construction of the state of the stat
LABEL DISPLAY NAME POLICY MARKING PROTECTION Image: Personal Global Global Image: Protection Image: Public Global Image: Protection Global Image: Protection Image: Public Global Image: Protection Global Image: Protection Image: Protection Global Image: Protection Image: Protection Image: Protection Image: Protection Global Image: Protection Image: Protection Image: Protection Add or remove labels Onfigure settings to display and apply on Information Protection end users Image: Protection Image: Protection Title Image: Protection Protection Protection Protection Protection
LABEL DISPLAY NAME POLICY MARKING PROTECTION Image: Personal Global Global Image: Personal Image: Public Global Image: Personal Global Image: Public Global Image: Personal Image: Personal Add or remove labels Image: Personal Image: Personal Image: Personal Image: Personal Image
Personal Global Public Global General Global Confidential Global Highly Confidential Global Add or remove labels Global Title Title
Public Global General Global Confidential Global Highly Confidential Global Add or remove labels Global Title Title
General Global Confidential Global Highly Confidential Global Add or remove labels Global onfigure settings to display and apply on Information Protection end users Title
Confidential Global I Highly Confidential Global Add or remove labels Global Title Title
Highly Confidential Global Add or remove labels onfigure settings to display and apply on Information Protection end users Title
Add or remove labels onfigure settings to display and apply on Information Protection end users Title
Configure settings to display and apply on Information Protection end users Title
Title
Sensitivity
Denotes and
poltip
The current label for this content. This setting identifies the risk to the business if this content is shared with unauthorized people inside or outside the organization.

Deploying AIP Clients

- The AIP client for Windows is a client for organizations that use Azure Information Protection to classify and protect documents and emails
- AIP client also has a viewer for organizations that don't have their own information protection infrastructure but want to consume protected content
- The stand-alone Azure Information Protection viewer app is available for Windows, Mac, Windows Phone, Android and iOS
- Rolling out the client is possible through Windows Update because it is included as both an executable (.exe) and a Windows Installer file (.msi) in the Microsoft Update catalog



Install the Azure Information Protection unified labeling client (AzInfoProtection_UL) for labels that can also be used by MacOS, iOS, and Android, and if you don't need advanced features such as user-defined permissions, HYOK, or the scanner. Install the Azure Information Protection client (AzInfoProtection) if you need advanced features that aren't yet available in the unified labeling client.

Configuring Automated Labeling

- The automatic labeling feature can assign labels to documents, files, and emails without user interaction when configured conditions are fulfilled
- Automatic labeling consists of:
 - Conditions for applying labels automatically
 - Automatic processing and recommendations for emails with attachments
 - The on-premises Azure Information Protection scanner to label local documents and files
- The automatic labeling requires an Azure Information Protection Premium P2 license, which is included in the license bundle Enterprise Mobility + Security E5

Configure conditions for automatically applying this label 🚯

If any of these conditions are met, this label is applied

CONDITION NAME	OCCURRENCES
Credit Card Number	1
EU Driver's License Number	1
EU National Identification Number	1
EU Passport Number	1
EU Social Security Number (SSN) or Equiv	1
EU Tax Identification Number (TIN)	1
+ Add a new condition	

Select how this label is applied: automatically or recommended to user

Add policy tip describing to users the reason for applying this label

It is recommended to label this file as Confidential \ Sensalari Internal

Configuring a Super User

- The Super User feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects
- The Super User feature is a feature to access all protected content of your tenant
- By default, the super user feature is not enabled
- The Super User is configured with the PowerShell cmdlets from the AADRM module
- You use Enable-AadrmSuperUserFeature cmdlet to enable this feature

Implementing Bulk Classification

- The Azure Information Protection scanner is a tool for automatic labeling and classification of files and documents from on-premises file shares and SharePoint servers
- The Azure Information Protection scanner can work as an extension to a Windows Server File Classification Infrastructure (FCI)
- The scanner is installed on a Windows Server with access to the on-premise environment containing the file shares and SharePoint libraries to label



Unified labeling across Office 365, Azure and Windows Information Protection

Centralized management

Configure and manage labels across apps and services in Office, Azure and Windows – all from the Security & Compliance Center

Unified classification

Uniform content classification to protect and preserve data across Office, Azure, Windows

Consistent across M365 & extensible to 3rd party

Consistent integration and experience across M365 apps & services. Extensible to 3rd party apps & solutions



Data protection & data governance go hand-in-hand

Unified approach to discover, classify & label

Automatically apply policy-based actions

Proactive monitoring to identify risks

Broad coverage across locations





What is a sensitivity label? Tag that is customizable, in cleartext, and persistent.

It becomes the basis for applying and enforcing data protection policies.



In files and emails, the label is persisted as document metadata



In SharePoint Online, the label is persisted as container metadata



Office 365 Message Encryption

Secure communication with anyone...



...on any device, in any email client



Secure enterprise productivity with Office 365 Advanced Threat Protection

Exchange EOP and Office 365 ATP

- Microsoft 365 tenants that have mailboxes hosted in Exchange Online rely on the Exchange Online Protection (EOP) service to route inbound and outbound mail
- Together, EOP and Microsoft 365 ATP provide a complete solution for protecting users against cyberthreats originating in email
- Advanced Threat Protection (ATP) extends the protection provided by EOP by filtering targeted attacks that could pass through EOP's line of defenses, including advanced threats such as zero-day attacks in email attachments and Office documents, and time-of-click protection against malicious URLs

The Anti-Malware Pipeline in Microsoft 365

- 1. Before mail enters the Microsoft 365 network and is processed by EOP, techniques such as IP and sender reputation, combined with heuristics
- 2. After that, it is scanned by multiple signature-based anti-virus scanners
- 3. Next, EOP scans individual files using a reputation block
- 4. Heuristic clustering is used to identify mail as suspicious simply based on an analysis of delivery patterns
- 5. Once these signals are collected, the results are run through a machine-learning (ML) model
- 6. If Microsoft 365 Advanced Threat Protection (ATP) is enabled in the tenant, ATP extends the protection of EOP



How ATP expands protection provided by EOP

Once email passes through the frontline defenses provided by EOP, it is further analyzed by ATP's Safe Attachments and Safe Links features for anything suspicious



Safe Attachments

- Safe Attachments is a feature in Microsoft 365 ATP that opens every attachment of a supported file type in a special hypervisor environment, checks to see if the attachment is malicious, and then takes appropriate action
- Safe Attachments will analyze attachments that are common targets for malicious content
- Selecting attachments to test
- Attachment testing

Safe Attachments Policy Options

ATP Safe Attachments policy options:

- Off
- Monitor
- Block
- Replace
- Dynamic Delivery
- Enable redirect

Safe Links

- Safe Links is a feature in ATP that protects users from malicious URLs that are commonly used in phishing attacks to extract sensitive information from a user
- When a user clicks a link in a message or document, Safe Links checks to see if the link is malicious by redirecting the URL to a secure server in the Microsoft 365 environment that checks the URL against a block list of known malicious web sites



Safe Links Policy Options

ATP Safe Links policy options:

- Block the following URLs
- Office 2016 on Windows
- Don't track when users click ATP safe links
- Don't let users click through ATP safe links to original URL
- Use Safe Attachments to scan downloadable content
- Apply safe links to messages sent within the organization
- Do not track user clicks
- Do not allow users to click through to original URL
- Do not rewrite the following URLs

End-User Experience with Safe Attachments

Getting SubKeys



CaReply CaReply All Groward MIM Thu 9/29/2016 2:52 PM Wayon Blair < admin@AtpTest1.onmicrosoft	t.com>
To O Dirk Xanthopoulos	
ATP Scan In Progress Outlook item	
Suggested Meetings Action Items	+ Get more add-in:
Hey Dirk, Check out the newsletter I attached from Contoso I men stuff:	tioned on the phone. This is great
 New Headquarters building is open. We should They are holding a 5K on Oct 1. Let's do it. Looks like it is time to renew our healthcare ben 	meet for lunch there!! efits again.

Let me know as soon as you get this!!

End-User Experience with Safe Links

Safe Links works in email by executing following steps:

- 1. Someone sends a user an email message that contains a URL to a web site.
- 2. The message flows through the anti-malware pipeline, and assuming it passes through all the initial checks, it eventually arrives in the recipient's inbox.
- 3. The user opens the message and clicks the link.
- 4. When the user clicks the link, the URL is redirected to a secure server that checks the URL against a block list of known malicious web sites.
 - 1. If the link is safe, the user's browser navigates to the target web site.
 - 2. If the link is malicious, the user's browser displays a warning page.

Securing the end user

- Critical to combating phishing and social engineering related attack vectors.
- Native protection built right into Office 365.
- Strong complement to your end user awareness and security training.
- Protection that extends to collaboration scenarios across desktop, web/online, and mobile clients.







Summary of New Office 365 ATP Safe Links Warning Pages for time-of-click protection

Securing your productivity scenarios:

Office clients and Office online

10:20 4	\leftrightarrow \rightarrow \circlearrowright \Leftrightarrow \Rightarrow	ttps://microsoft-my.sharepoint-df.com/w///personal/sumitm_microsoft_com1/_layouts/15//Doc.aspx?sourcedoc=%78ADFD9908-583E-	*	
SWOTAnalysisMay2018	III Word Online Summe Summe File Home Insert Layo €) ∨ ⊕ of Catleri (Body)	athetra > XTP Demo Docs. SWOTAnalyzisMay2018 - Saved ● Simpl nut References. Review View Help DocuSign Open in Word Q Tell me what you want to do v 11 v A A B I U ∠ A A A B . I U ∠ A A A A B I U		This website has been classified as malicious.
10:29 <i>√</i> ◀ Word	l∎ ≎ lu.	John Doe aric street, redmond, wa		
anam06.safelinks.protection	a.outlook.co C	Poge Brask	Opening thi	s website might not be safe.
This website has i classified as malie	been cious.	SWOT Analysis: You can include sWOT analysis by completing the basis below to assess your business in the current environment in terms to strongiths and weaknesses (internal) is and opportunities and threats (external). This is a good exercise to go through on an annual basis. After completing your	http://spamlink	.contoso.com
Identified Withold with Opening this website might not be sa Hey //pening this website might not be sa Hey //pening this website might not be sa Hey //pening this website might not be sa	fe.	analysis, provide your broughts on: how your strengths can help you to maximize opportunities and minimize threads; how your weaknesses can slow your akility to capitalize on the opportunities; and how could your weaknesses expose you to thread? • Anamage • Anamage	We recommend be safe and could personal data.	that you don't open this website, as opening it might not d harm your computer or result in malicious use of your
Not if address for can have a set of the set	vection	 Aust, spedie Aust, spedie Construction Const	X Close this page	ре
Average Anner		Area to improve Nor express to the second sec	Continue anyway (not recommended)
Open		New invocations New partnerships Regratmenships Strengths: What will be your company's strengths when you launch? How do you see this changing	Powered by Onice	202 Auvalicer Initer Frotection
Сору	<u>м</u> –	In the future? • Weaknesses: If you were the competition, what would you say to prospective customers about where your company's products or services are weak or deficient? What are the most important weaknesses to overcome first?		
Edit		Opportunities: Whin product improvements or new partnerships, where could your business grow? What new segments could you enter in the future? Theats: What network later could put pressure on your business growth or cash flow? Which of these threats can you control? Which ones can't you control?		
Cancel		······	Footer	
	Page 2 of 2 186 words English (U.S.)	Inner Ring (Fastfood) : FF1	100% Help Improve Office	

Word iOS client showing **Office 365 ATP Safe Links** block from a click within a document.

Word Online showing Office 365 ATP Safe Links block from a click within a document.

Securing your collaboration scenarios:

SharePoint Online, OneDrive for Business and Microsoft Teams

9:52 1	ail lte 🗩	← C ▲ Secure https://o	365tiscHv2 my shares	point.com	personal/aumitm_o365fit6fiv2_onmerosoft_com	n/_layouts/15/o	nedrivit impa	_	_	_
Search	<u></u>	, Search everything	Del	lete	iestu i suzu i a					
\leftarrow		Sumit Malhotra		άđ.	test03082018		March 8	Sumit Malhotra		# ⁸ Shared
		Files		10	Test09142017		September 23, 2017	Sumit Malbotra		Private
		Recent		int i	Test09152017		September 23, 2017	Sumit Malhotra		Private
		Recycle bin		10	Test09162017		September 23, 2017	Somit Malhotra		Private
		Contoso	+	10	Test09182017		September 23, 2017	Sumit Malhotra		Private
		IRM Protected Test		in i	TEST09192017		September 23, 2017	Survit Malhotra		Private
	20 March 12 540 10 200			nt	Test09202017		September 23, 2017	Sumit Malhotra		R ^R Shared
This file is compro	mised by malware. To protect your			ist.	Test09212017		September 23, 2017	Sumit Malhotra		Private
and other comma	nds. Contact your admin for options			st.	Test09222017		September 23, 2017	Sumit Malbotra		R ^B Shared
or learn more.				10	Test09262017		September 26, 2017	Sumit Malbotra		it Shared
File name	SOW_Contoso_April_2018.docx			in i	Test10092017		October 9, 2017	This file is con	promised by	×
				uff.	Test10102017		October 10, 2017	To protect your PC and o	ther files, we've remove	d Open, Share, and other
Modified .	Jun 13			int i	Test10202017		October 20, 2017	commands. Contact you	r admin for options o <mark>r le</mark>	sam more.
				10	Test10232017		October 23, 2017			ок
Size	I KB			10	Test10252017		October 25, 2017	Sumit Malhotra		Private
	ODfR Malwara Tast			iff.	URL Test		February 21	Sumit Malhotra		Private
Location				a)	doclib_test.pptx		December 4, 2017	Sumit Malhotra	1000 bytes	i ² Shared
Shared with					hyderabad biryani.txt		September 27, 2017	Sumit Malhotra	242 bytes	Private
			0	B	Invoice for approval.pdf		September 25, 2017	Sumit Malhotra	199 KB	i ^p Shared
Has access from "	SOW_Contoso_April_2018"			a	Test.docx		September 23, 2017	Sumit Malhotra	10.7 KB	n ^e Shared
				٥	test_odb_12042017.docx	0	December 4, 2017	Sumit Malhotra	1000 bytes	n ^e Shared
				61	ThisInvoiceNeedsApproval 092		December 4, 2017	Sumit Malbotra	1000 bytes	i ⁸ Shared

OneDrive iOS app showing files detected and blocked by <u>Office 365 ATP</u>

SharePoint Online WebUX showing files detected and blocked by Office 365 ATP



Microsoft Teams desktop client showing files detected and blocked by <u>Office 365 ATP</u>

Securing your collaboration scenarios:

Office 365 ATP Safe Links protection in Microsoft Teams



Malicious URL in conversations from Guest/External user in Teams desktop client

Office 365 ATP blocks a malicious link click from Teams desktop client

-Microsoft 365

Grazie