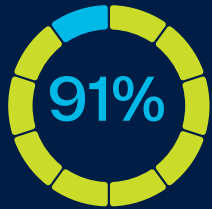


Prevent hacked Azure consumption



91% of attacks are coming from a phishing email >



We all know hackers have been creative in their operations. The last couple of months, multiple cloud environments have been hacked with an unusual high consumption invoice as a result.

Be aware that 91% of the attacks are coming from phishing emails, working as follows:



Potential actions you can do to prevent attacks:

- Review which users, tenants, and subscriptions are at risk within the Azure portal.
- Review any other Azure resources or services that may have been unexpectedly provisioned in the last week(s).
- Suspend any suspicious Azure resources or Azure subscriptions.
- As a precaution, we highly recommend that all global admins in your customer's tenant immediately change their passwords if they haven't done so already.
- Review and verify all global admin user password recovery emails and phone numbers within Azure AD, and update if necessary.



Some concrete action points to prevent Phishing can be found below.

Access

Basic checks to make for end user Microsoft environments:



✓ Check user access rights

- Is your list of users up to date?
- How often do you refresh/Update user access rights?
- Are all users trained to spot phishing attacks?
- How many users have Global Admin Rights? (Microsoft officially recommends only having 2-4 Global Administrators)
- Are your Global Administrators trained?
- What level of security checks do you have in place? (Tools/Monitoring & Blocking)
- Password less access – Windows Hello
- MFA

✓ Device management

- How are all devices secured?
- Are all devices up to date?
- Security policies?

✓ Zero Trust

- Adopt a Zero Trust model for better resilience against future attacks by using the [Microsoft Zero Trust Quiz](#) to get quick start recommendations.

Reminding all cloud users about the [shared responsibility](#) model from Microsoft.

What tools are there to aid defence?

• SecureScore

Evaluate your current security posture and identify potential improvements across all your Microsoft 365 workloads with centralized visibility from Secure Score.

• Microsoft Defender for Office 365

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools like Teams & SharePoint.

• MFA

Multifactor authentication (MFA) adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone.

• Microsoft Defender for Cloud

Defender for Cloud is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms.

• Sentinel

Microsoft Sentinel is a scalable, cloud-native, security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.



Monitoring & Blocking

• Azure Cost Management

Azure Cost Management has an alert feature. Alerts are generated when consumption reaches a threshold. If you want to create Azure budgets, see [this article](#).



Microsoft's Best Practices



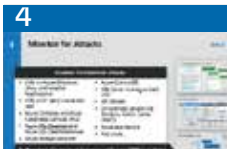
1
Operationalize
Secure Score for
cleaning up risk



2
Passwordless or
MFA for admins



3
Enterprise
segmentation & zero
Trust preparation



4
Enable Threat
Protection for Azure
Resources



5
Follow guidance to
secure your DevOps

What we offer

Education

- ✓ • Security Awareness Program

✓ Pre-built Click-to-Run solutions

- Secure Score
- Sentinel
- Cloud Backup
- Ransomware

✓ Security Professional Services

- Teach me
- Do it for me
- Help me

✓ BPA team

- Running a bot against our MSFT PACs
- Accessing customer set-ups to check for an MFA flag

Two actions that secure you better in the short term:

1 Mandatory to use MFA for Admin functions

2 Threshold in Azure Cost Management

Documents for more information:

Next gen pdf >

Ransomware >

Protect your Azure
customer >

Azure cost
management >

Interested in solutions for the
long run?

Contact your local TD SYNnex office