

Uzņēmuma darbinieku pikšķerēšanas tests izmantojot Microsoft Defender for Office 365

17.03.2026

**Gatis Pabērzs
Information Security Manager,
Clear Junction Group**

SIMULĒT ? NESIMULĒT



From: Account Department <ACCOUNTS@...COM>
Sent: 21 December 2022 09:15
To: [Redacted]
Subject: File MM Expenses Report.xlsx Has Been Shared with [Redacted]

MM Expenses Report.xlsx has been shared with you

Let me know if you'd like to review it together. Thanks!



This link will work for [Redacted]@...com

Open

[Privacy Statement](#)



Sign in

Email, phone, or Skype

[No account? Create one!](#)

[Can't access your account?](#)

Next



← `{{loginUser}}`

Enter password

Password

[Forgot password?](#)

Sign in



Rezultāts pēc pirmā gada



Vidēji ceturksnī akreditācijas dati ir sniegti 1465 reizes.

Vienu reizi sniegti akreditācijas dati - 3818 lietotāji

Divas reizes sniegti akreditācijas dati - 737 lietotāji

Trīs reizes sniegti akreditācijas dati - 118 lietotāji

Četras reizes sniegti akreditācijas dati - 11 lietotāji

IT



Simulated	Passed	% Passed	Clicked	Clicked %	Compromised	Compromised %
395	287	73%	108	27%	44	11%
395	287	73%	108	27%	44	11%

Lai pārietu tieši uz uzbrukuma simulācijas
apmācību, izmantojiet:
<https://security.microsoft.com/attacksimulator>

Nepieciešmā licence:
Microsoft 365 E5 vai
Microsoft Defender for Office 365 Plan 2

Dokumentācija:
<https://learn.microsoft.com/en-us/defender-office-365/attack-simulation-training-get-started>



<https://techcommunity.microsoft.com/blog/microsoft-security-blog/announcing-attack-simulation-training-read-apis---now-in-beta/2821787>

<https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/introducing-the-release-of-attack-simulation-training-write-api-functionality/3812297>

The screenshot shows the Microsoft Power Query Editor interface. The main window displays the M code for a query named 'Query1'. The code is as follows:

```
let
    token_uri = "https://login.windows.net/" & #"Azure AD Tenant ID" & "/oauth2/token",
    resource="https://graph.microsoft.com",
    tokenResponse = Json.Document(Web.Contents(token_uri,
    [
        Content = Text.ToBinary(Uri.BuildQueryString(
            [
                client_id = #"Azure Application Client ID",
                resource = resource,
                grant_type = "client_credentials",
                client_secret = #"Azure Application Client Secret"
            ]
        )),
        Headers = [Accept = "application/json"], ManualStatusHandling = {400}
    ])),
    access_token = tokenResponse[access_token],
    Source = OData.Feed("https://graph.microsoft.com/beta/security/attackSimulation/simulations?$select=id, displayName, description, attackType, payloadDeliveryPlatform, attackTechnique, status, createdDateTime, lastModifiedDateTime, launchDateTime, com
    #\"Expanded createdBy\" = Table.ExpandRecordColumn(Source, \"createdBy\", {\"displayName\", \"id\", \"email\"}, {\"createdBy.displayName\", \"createdBy.id\", \"createdBy.email\"}),
    #\"Expanded lastModifiedBy\" = Table.ExpandRecordColumn(#\"Expanded createdBy\", \"lastModifiedBy\", {\"displayName\", \"id\", \"email\"}, {\"lastModifiedBy.displayName\", \"lastModifiedBy.id\", \"lastModifiedBy.email\"})
in
    #\"Expanded lastModifiedBy\"
```

On the right side of the interface, a table of results is displayed with the following columns: 'id', 'displayName', 'description', 'attackType', 'payloadDeliveryPlatform', 'attackTechnique', 'status', 'createdDateTime', 'lastModifiedDateTime', and 'launchDateTime'. The table contains three rows of data:

id	displayName	description	attackType	payloadDeliveryPlatform	attackTechnique	status	createdDateTime	lastModifiedDateTime	launchDateTime
4529c613-ec...							11/11/2023 17:30	09/11/2023 17:30	email
295df21c-d5...							11/11/2023 17:01	09/11/2023 17:00	email
d98c2c5a-ec...							11/11/2023 16:31	09/11/2023 16:30	email

Q&A

The background features a diagonal split between a light cream color (top-left) and a medium blue color (bottom-right). A vertical red line runs along the right edge of the slide, separating the blue area from a darker blue area on the far right.

Paldies!

g.paberzs@clearjunction.com

www.linkedin.com/in/gatispaberzs/