Tölvuárásir með phishing póstum og varnir gegn þeim

Guðmundur Pétur Pálsson

Microsoft ráðgjafi

Opin Kerfi

From: Þorsteinn G. Gunnarss
Sent: föstudagur, 25. ágúst 2
To: Ágústa Rósa Finnlaugsdót
Subject: Flytja Brýn

Kæri Ágústa

Getur þú sent greiðslu til Ítalí

Með kveðju
Þorsteinn G. Gunnarsson

From: Þorsteinn Guðlaugur Gunnarsson [mailto:iphone_access@aol.co.uk]
Sent: miðvikudagur, 9. maí 2018 07:46
To: Ágústa Rósa Finnlaugsdóttir <rosa@ok.is>
Cc: Guðrún Jónsdóttir <gudrun@ok.is>
Subject: Flytja

Góðan dag
Getur þú sent 14,500,00 evrur til Englands í morgun?
Hvaða bankagögn ætti ég að senda?

Með kveðju
Þorsteinn Guðlaugur Gunnarsson

Sent úr iPhone-inum mínum

ation Fri,

, we

d party.
your
rstand
ur

participating online stores.

Activate Now for Verified by Visa

Thank you for your support.
Visa Service Department

***DON'T WAIT! The Link Above Expires on 12/28!

h on the limitation, please let us know by going to the Help Centre and click *Contact Us*.

Upin Kerfi

Hvernig verjum við gögnin okkar í heimi þar sem;

58 % einstaklinga hafa óvart sent viðkvæmar upplýsingar á rangan aðila

81% innbrota í fyrirtæki er vegna veikra eða stolinna lykilorða

300K spillihugbúnaðar (malware) útgáfum er dreift hvern dag

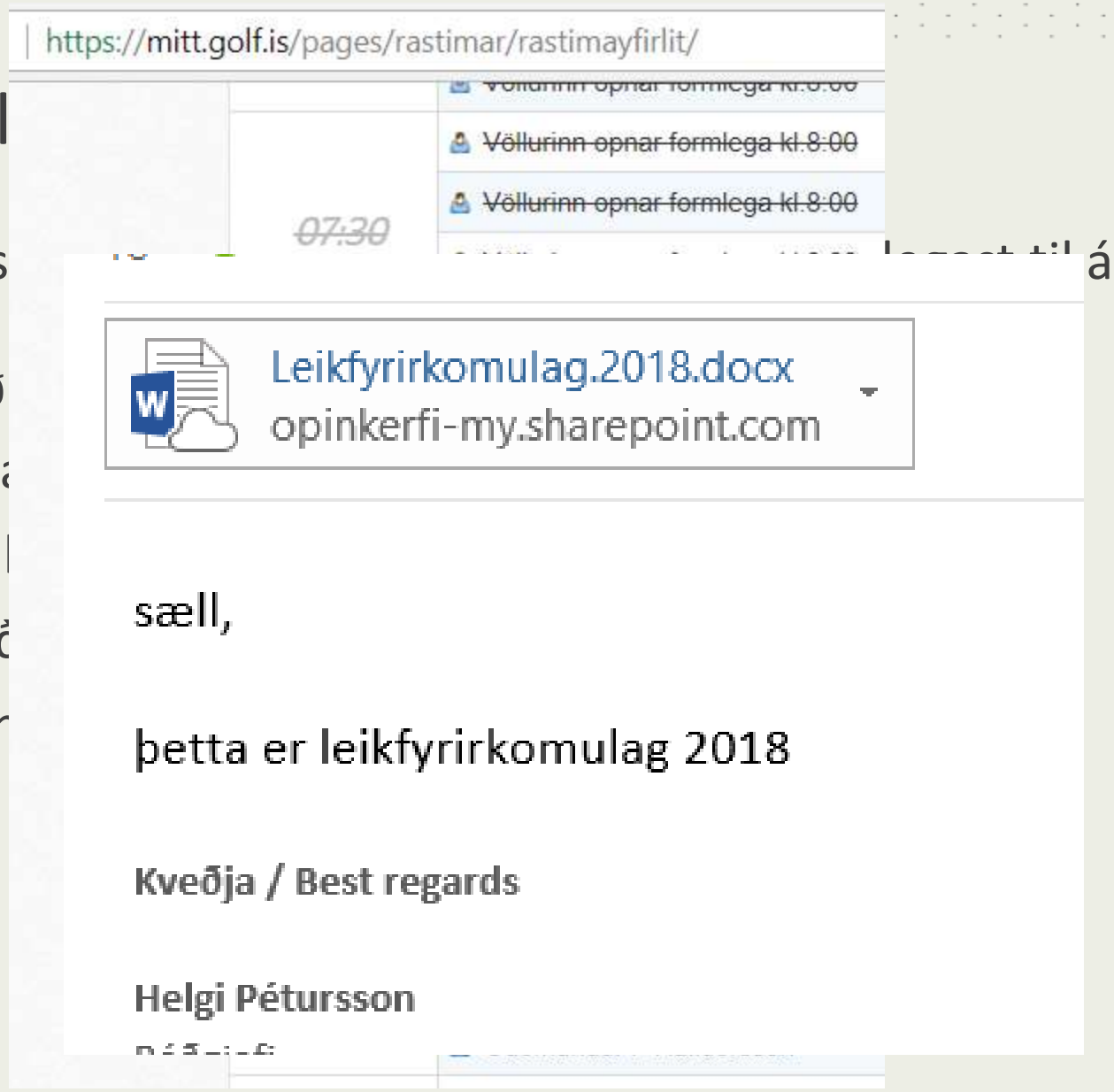
Opin Kerfi

Secure https://www.golfmyndir.is/2015/MeistaramotGR2015/Dagur6/i-9bx48fP

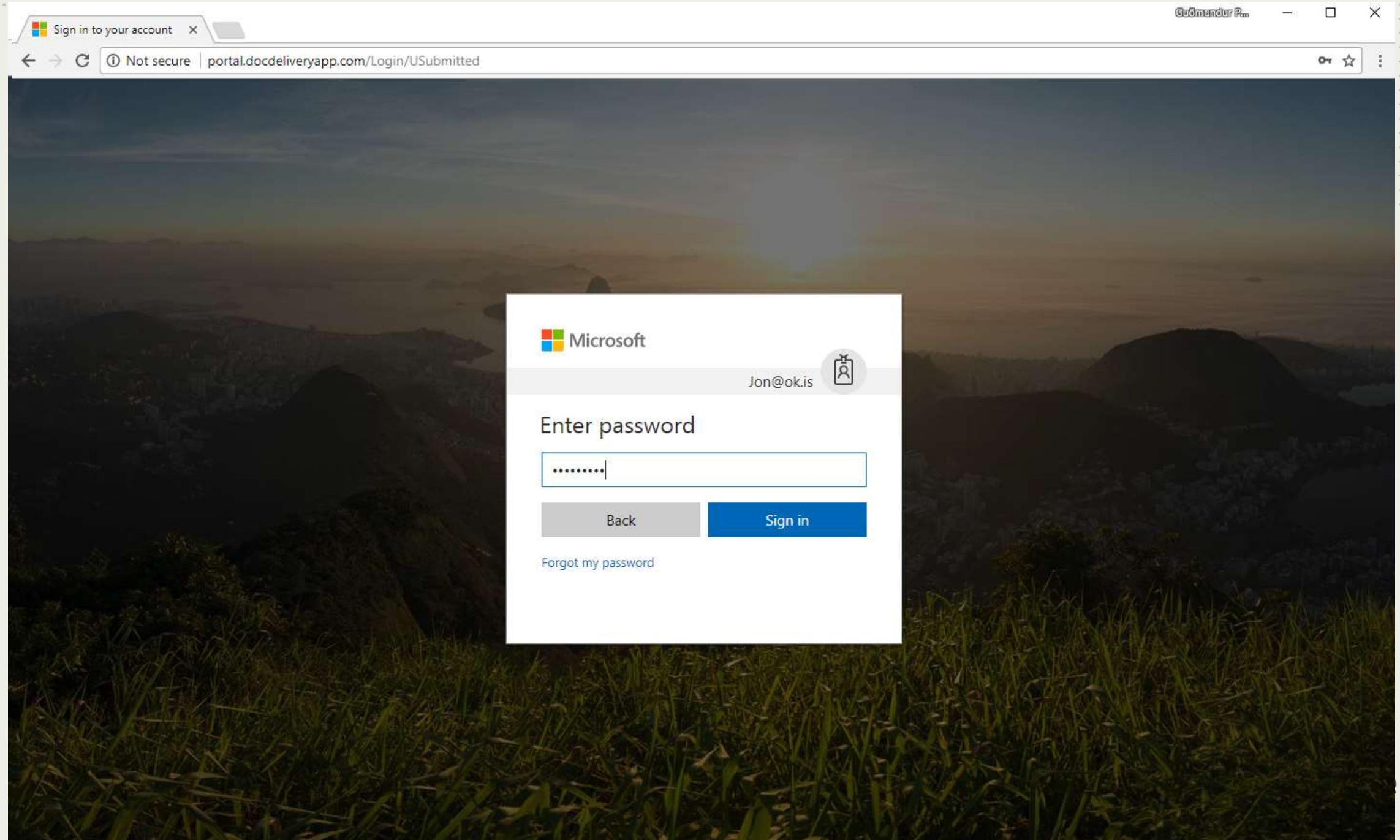
Þorsteinn G. Gunnarsson með vipp við 2. flöt.

Nálgunar til

- Phishing pós
  skoðun)
  - Oftast til að
- Vinabeiðnir
- Senda inn fa
- Póstar um a
- Hafa sambar



Opin Kerfi


Sign in to your account
Not secure
portal.docdeliveryapp.com/Login/USubmitted
Microsoft
Jon@ok.is
Enter password
Back
Sign in
Forgot my password

- Er kc
- Logg
- Les c
- Íslen
- Hefu
- Auð

Opin Kerfi

- Í pósti finnur hann eitthvað áhugavert
- Annan aðila til að reyna að nálgast
- Upplýsingar um greiðslu sem er á leiðinni
- Upplýsingar um reikninga (miklar líkur á að yrðu jafnvel samþykktir sjálfkrafa)

Fyrirtæki er að selja vöru til nýs viðskipavinar

- Hakker býr til reglu í
- Kynnir sér innihald h
- Áttar s
- Sendir
- Núna
- Hakke
- Tveim
- Hakke
- Býr til
- Semur
- Jafnvel þó kaupand
- Og millifærslan fer til hakkarans.....

nda

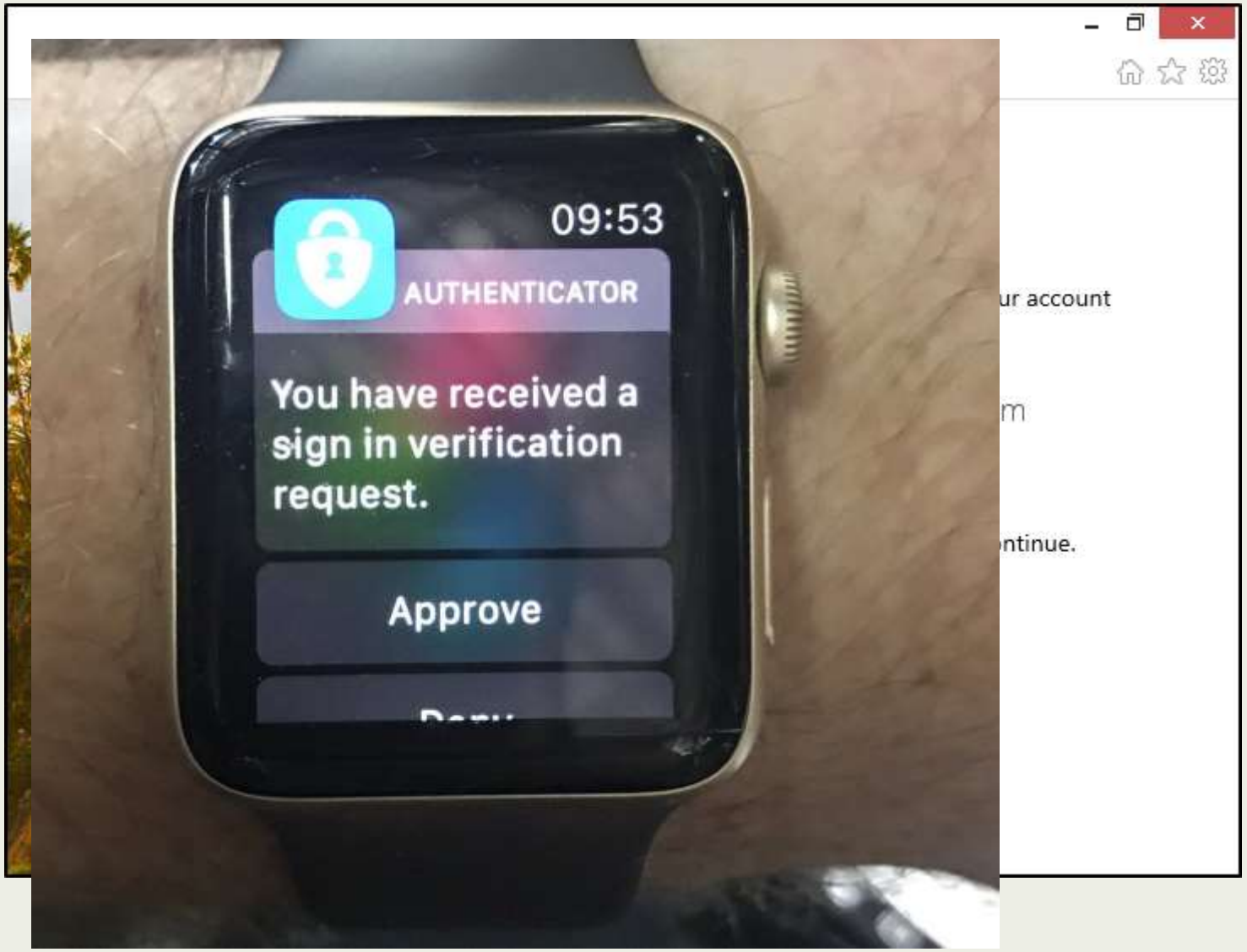
ið uppl. um

í pósthólfinu

rningu í pósti til
notanda B um hvort aldrei þann
póst heldur bara hakkerinn sem svarar um hæl

Opin Kerfi

Hvað er til ráða?



Opin Kerfi

Hvað er til ráða?

- Uppfærslur
  - Allar útstöðvar að keyra nýjasta stýrikerfið, með nýjustu öryggisuppfærslum
  - Allir netþjónar að keyra nýjasta stýrikerfið, með nýjustu öryggisuppfærslum
  - Vera með kerfi sem sér um uppfærslur og ástand uppfærslna (skýrslur)
- Varnir
  - Vírusvarnir – miðlæg stjórnun – eftirlit – sjálfkrafa viðbrögð
  - Gagnagíslatökuforrita varnir (Ransom ware)
  - Dulkóðum á diskum
  - Applocker.....
  - Hash varnir

Opin Kerfi

Hvar byrjum við?

- Netþjónum?
- Útstöðvum?
- Eldveggnum?
- Notendum?

Opin Kerfi

Notandinn er lykill að öryggi

- Byrjum á að vernda notandann (notanda kennið)
  - Tveggja þátta auðkenning
  - Lykilorð
    - 16 stafir +
    - Nota PIN, Windows Hello, fingraför í staðinn fyrir að slá inn lykilorð
  - Virkja eftirlit
    - Hvenær, hvaðan, inná hvað var notandaauðkennið skráð inn
    - Eðlileg hegðun – er tölvunotkun notandans eins og venjulega?
    - Notkun forrita
      - Hverjir hafa aðgang
      - Hvar eru gögnin
      - Hvaðan er verið að skoða þau
      - Hvaða forrit er verið að nota (shadow IT)

Opin Kerfi

Opin Kerfi

Hvaða lausnir eru í boði í 365?

EMS & O365, The cloud better together

	Cloud and hybrid identity management	Mobile device management	Information protection
Enterprise Mobility Suite	**Azure AD for O365** + • Single Sign on for all cloud apps • Advanced MFA for all workloads • Self Service group management and password reset with write back to on prem directory • Advanced security reports • FIM (Server + CAL)	**MDM for O365** + • PC Management • Mobile App Management (prevent cut/copy/past/save as from corporate apps to personal apps) • Secure content viewers • Certificate Provisioning • System Center integration	**RMS for O365 +** • Protection for on-premises Windows Server file shares ❖ Departmental templates ❖ Email notifications when sharing documents ❖ Email notifications when shared documents are forwarded
Office 365	**Basic Identity Mgmt via Azure AD for O365:** • Single Sign on for O365 • Basic Multifactor Authentication (MFA) for O365	**Basic Mobile Device Management via MDM for O365** • Device Settings Management • Selective Wipe • Built into O365 Mgmt Console	**RMS Protection via RMS for O365** • Protection for content stored in Office (on prem or O365) • Access to RMS SDK • Bring your own Key

Opin Kerfi

Proactive attack prevention and detection

Help your customers remain constantly aware of the current threat landscape to help identify attacks and attackers before they cause damage or disruption.

Risk assessment: Perform a security assessment analysis to help understand security risks, formulate policies and plan for improvement.

Manage mobile productivity: Secure access to the cloud helping to protect data on unmanaged devices.

Safeguard messaging: Deliver zero-day protection to help guard against unknown malware and viruses.

Detect and respond to suspicious activity: Use artificial intelligence and machine learning to help identify high-risk activity and quickly respond to contain attacks before damage occurs.

Protect, detect and respond to advanced threats: Uses artificial intelligence, machine learning, and other means to help prevent successful attacks, identify high-risk activity and quickly respond to contain attacks before damage occurs.

Microsoft 365

Windows 10	Office 365	Enterprise Mobility + Security
Secure devices with a comprehensive set of defenses and management capabilities that can help protect, detect and respond to advanced attacks	Reduce the threat of malicious content and help identify abnormal usage, security incidents, and threats	Protect user identities, help identify high-risk usage and guard against advanced attacks in the cloud and on-premises

Cloud App Security | Discover | Investigate | Control | Alerts 8

Activity map

over the last m

Trends

Activities | Active users

over the last w