Email-based threats: addressing the human factor

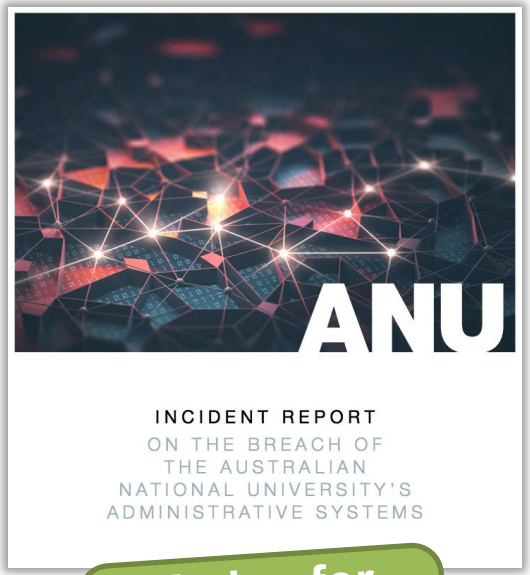
Sebastian Łopieński
CERN Deputy Computer Security Officer

CHEP 2019

24th International Conference on Computing in High Energy & Nuclear Physics

4-8 November 2019, Adelaide, Australia

Instead of “why”: a recent data breach at ANU



Kudos for being transparent!

Public detailed report (Oct. 2nd, 2019)

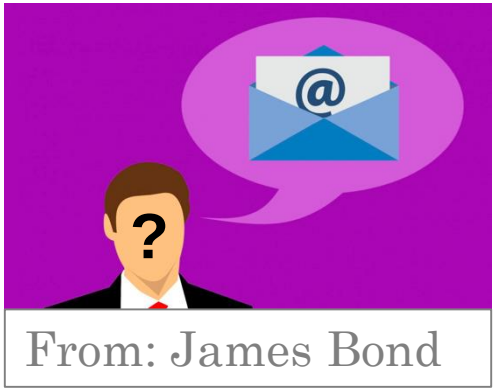
*“The initial means of infection was a sophisticated **spear phishing email** (targeting a senior staff member)*

[..]

*Information from victim’s calendar was used to conduct **additional spear phishing attacks** later in the campaign”*

E-mail is the main attack vector

E-mail is the main attack vector



It's very (too) easy and
cheap to send e-mails

It's trivial to **fake *"From"* field**

Malicious e-mails contain
infected attachments and
links to malicious websites

What tactics do adversaries employ?

From: Giovanni [redacted] <office.outlook@
Date: Monday, 10 December 2018 at 10:
To: [redacted]
Cc: [redacted]

[redacted]

Subject: Giovanni [redacted] has shared a

Please see the attached for your action

Regards
Giovanni [redacted]

Scan.pdf

10.12.2018, 20:37, [redacted]

Dear Giovanni,
I think this might be fishing !
Can you confirm ?
Thanks,
[redacted]

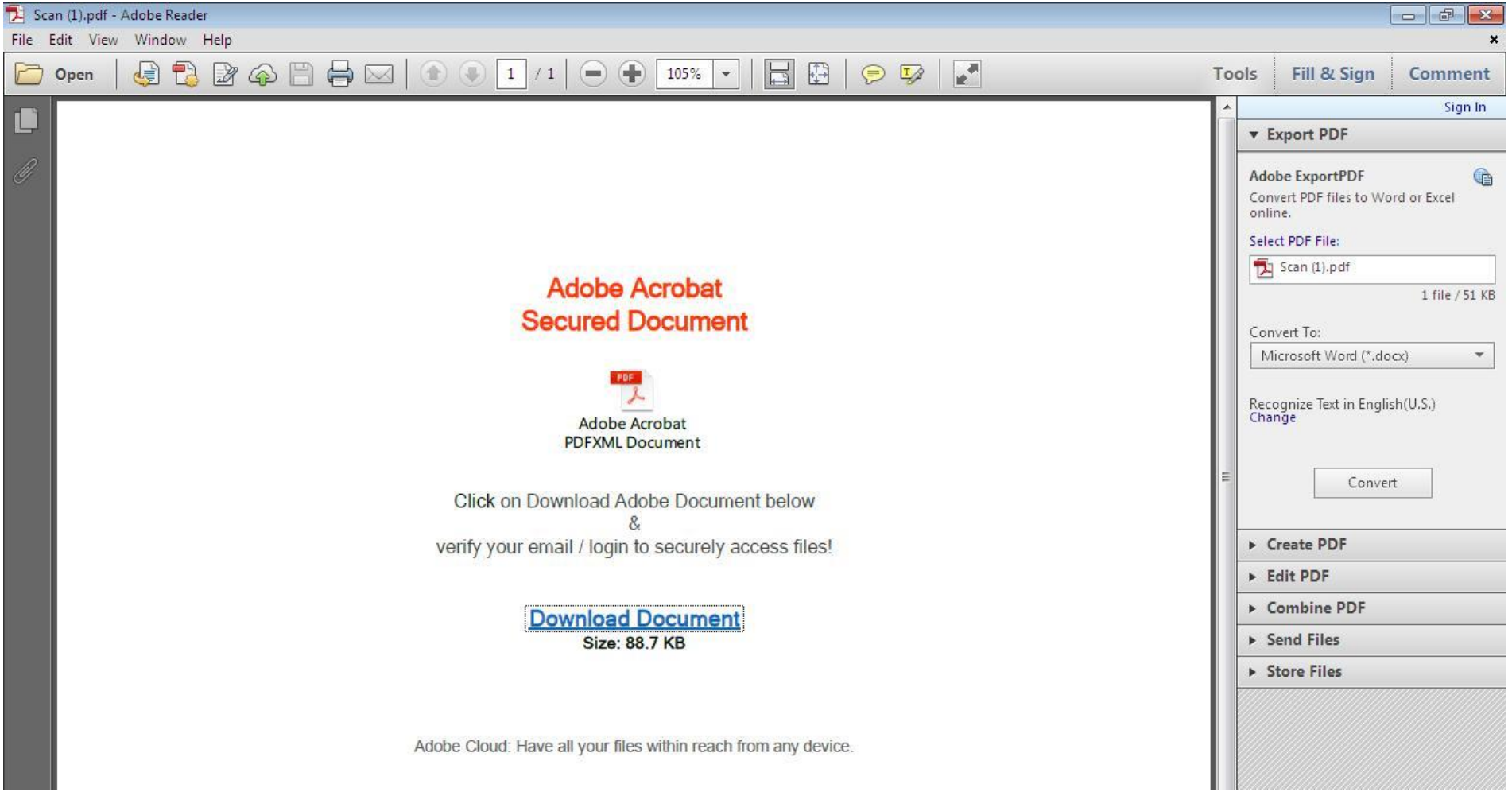
From: Giovanni [redacted] <office.outlook@yandex.com>
Date: 10 December 2018 at 10:42:14 CET

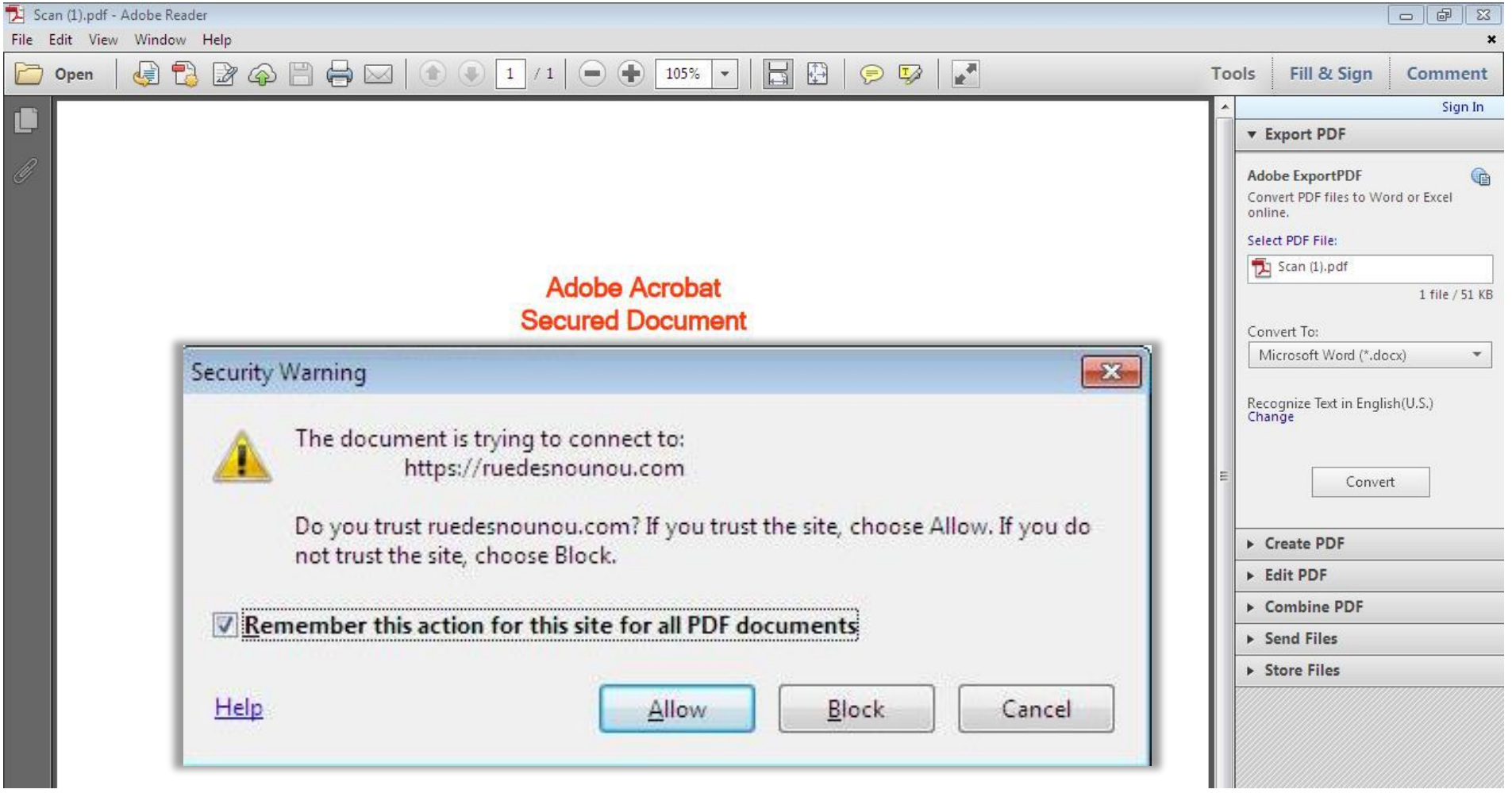
Hi [redacted],

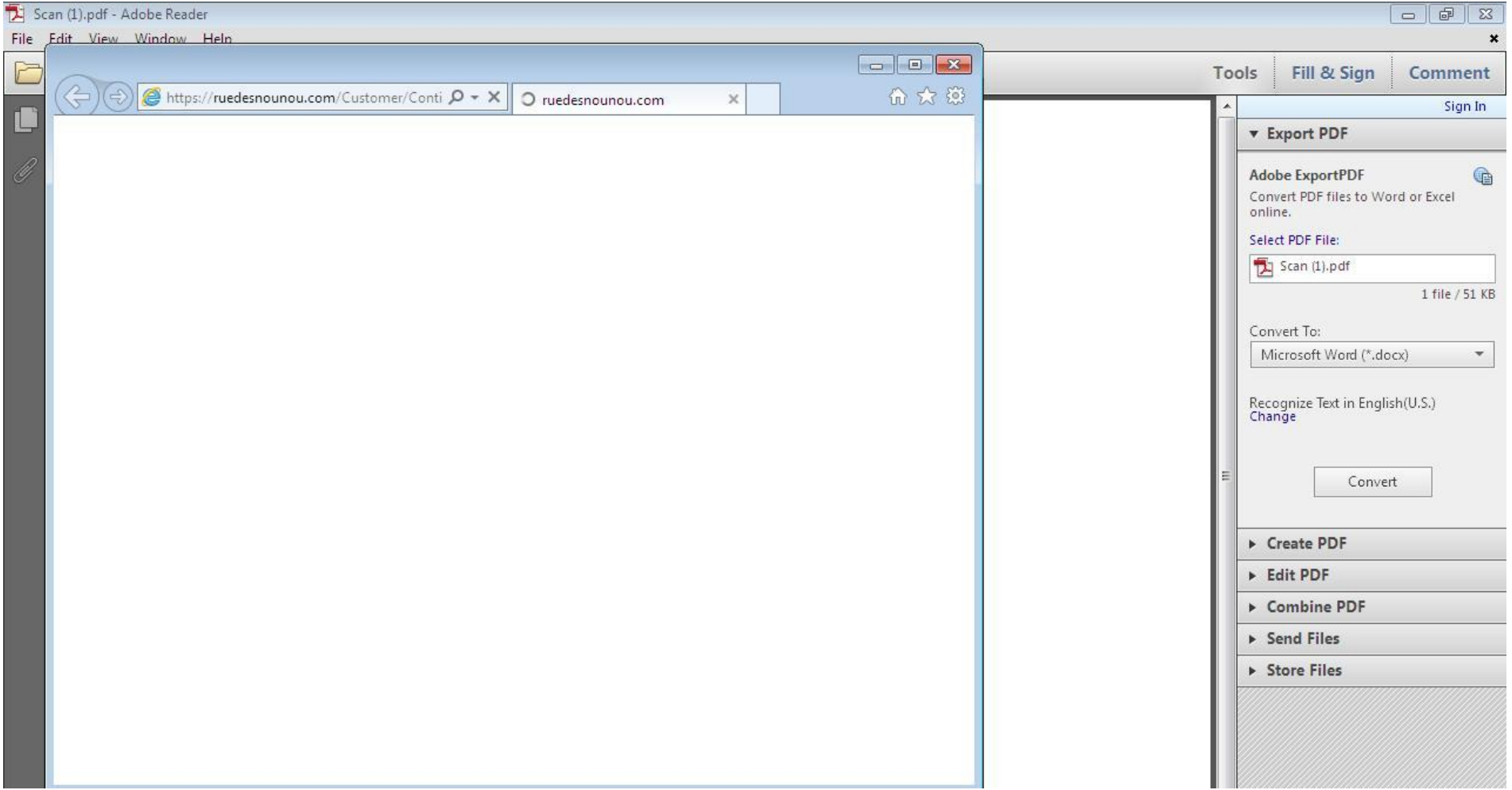
This is safe and secured to access

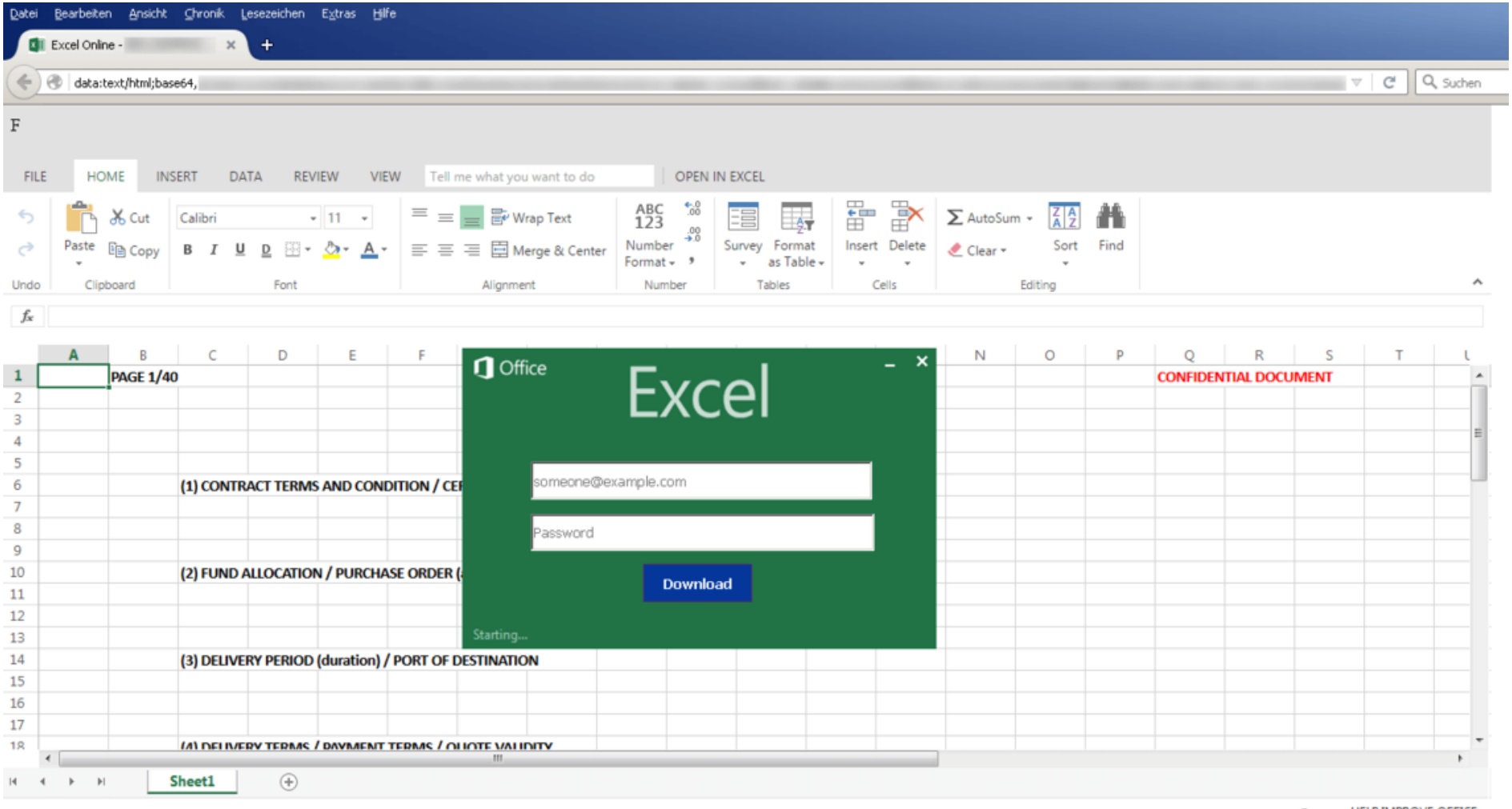
Get back to me soon as you get this .

Regards
Giovanni [redacted]


Scan (1).pdf - Adobe Reader
File Edit View Window Help
Open
1 / 1
105%
Tools
Fill & Sign
Comment
Sign In
Export PDF
Adobe ExportPDF
Convert PDF files to Word or Excel online.
Select PDF File:
Scan (1).pdf
1 file / 51 KB
Convert To:
Microsoft Word (*.docx)
Recognize Text in English(U.S.)
Change
Convert
Create PDF
Edit PDF
Combine PDF
Send Files
Store Files
Adobe Acrobat
Secured Document
Adobe Acrobat
PDFXML Document
Click on Download Adobe Document below
&
verify your email / login to securely access files!
Download Document
Size: 88.7 KB
Adobe Cloud: Have all your files within reach from any device.


Scan (1).pdf - Adobe Reader
File Edit View Window Help
Open
1 / 1
105%
Tools
Fill & Sign
Comment
Sign In
Export PDF
Adobe ExportPDF
Convert PDF files to Word or Excel online.
Select PDF File:
Scan (1).pdf
1 file / 51 KB
Convert To:
Microsoft Word (*.docx)
Recognize Text in English(U.S.)
Change
Convert
Create PDF
Edit PDF
Combine PDF
Send Files
Store Files
Adobe Acrobat
Secured Document
Security Warning
The document is trying to connect to:
https://ruedesnounou.com
Do you trust ruedesnounou.com? If you trust the site, choose Allow. If you do not trust the site, choose Block.
Remember this action for this site for all PDF documents
Help
Allow
Block
Cancel


Scan (1).pdf - Adobe Reader
File Edit View Window Help
https://ruedesnounou.com/Customer/Conti
ruedesnounou.com
Tools
Fill & Sign
Comment
Sign In
Export PDF
Adobe ExportPDF
Convert PDF files to Word or Excel online.
Select PDF File:
Scan (1).pdf
1 file / 51 KB
Convert To:
Microsoft Word (*.docx)
Recognize Text in English(U.S.)
Change
Convert
Create PDF
Edit PDF
Combine PDF
Send Files
Store Files


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Excel Online -
data:text/html;base64,
Suchen
FILE HOME INSERT DATA REVIEW VIEW Tell me what you want to do OPEN IN EXCEL
Undo Clipboard Font Alignment Number Tables Cells Editing
Paste Cut Copy Calibri 11 Wrap Text Merge & Center Number Format Survey Format as Table Insert Delete AutoSum Clear Sort Find
PAGE 1/40
CONFIDENTIAL DOCUMENT
(1) CONTRACT TERMS AND CONDITION / CE
(2) FUND ALLOCATION / PURCHASE ORDER (
(3) DELIVERY PERIOD (duration) / PORT OF DESTINATION
(4) DELIVERY TERMS / PAYMENT TERMS / QUOTE VALIDITY
Office
Excel
someone@example.com
Password
Download
Starting...
Sheet1
HELP IMPROVE OFFICE

… half a year later …

Giovanni [redacted] <angelavidos340@gmail.com> 19 June 2019 at 12:33

Respond

To: [redacted]@cern.ch>

[redacted],

Let me know when you are available. There is something I need you to do.
I am going into a meeting now with limited phone calls, so just reply my email.

Giovanni

Sent from my iPad

… and another 4 months later

Giovanni **<lindajeff99@aol.com>** Junk - CERN Yesterday at 17:13

URGENT

To: @cern.ch>

I am planning a surprise for some of the staffs with gifts. I need you to get a purchase done, I'm looking forward to surprise some of the staffs with gift cards,I count on you to keep this as a surprise pending when they received it,I need 10 pieces of Amazon $100 face value each gift cards. I need you to get the physical card, then you scratch the card take a picture of the cards pin,attach and email it to me. How soon can you get this done ?
I will Reimburse you back later....

Regards
Giovanni

Advanced techniques used by criminals

- Spear phishing: malicious mails targeted at specific individuals
  - crafted using information gathered earlier: project names, colleagues names, hierarchy, who is on holidays etc.
  - sent “from” a colleague, a business partner, even the boss
  - “whaling” attacks – targeting top management

- Using “contacts” lists: An attacker compromises mailbox of a victim, and sends malicious e-mails “from” the victim to their contacts

- Joining existing conversation: An attacker compromises mailbox of a victim, and replies to existing conversations, adding a malicious URL or attachment

How can we defend ourselves and our users?

Technical protection measures (simplified view)

- Traditional **anti-spam filters** (signature-based, blocking certain file types etc.)
- Advanced **anti-malware systems** (behavior-based)
  - "detonating" (opening) attachments in a controlled environment
  - (???) visiting embedded links – very problematic!
- **Hardened end-points computers**, for example:
  - anti-virus software, secure browsers etc.
  - macros disabled in received documents
  - not running as administrator
- **Network protection and detection**
  - e.g. blocking malicious domains at the DNS level
  - only partially effective (computers on the corporate network, no DNS over HTTPS etc.)

Despite these measures, some malicious e-mails will reach users

Users are our last line of defense

Simulated phishing campaigns at CERN

Goal

raising awareness
+
understanding
the scale of the problem

Approach

no spear phishing

no internal knowledge

no blaming

Techniques

“malicious” links
(2016-2018)

“malicious” attachment
(2019)

Various messages, senders, sender domain etc.

Sonia Abelona <Sonia.Abelona@cern.org>

Sonia Abelona has shared a file with you

To: [redacted]

Dear [redacted]

Please see the attached for your 2019 contract amendment request.

Regards
Sonia Abelona
Manager at Human Resources

Contract amend...21.doc

Federico Campesi <Federico.Campesi@cem.ch>

Federico Campesi has shared a file with you

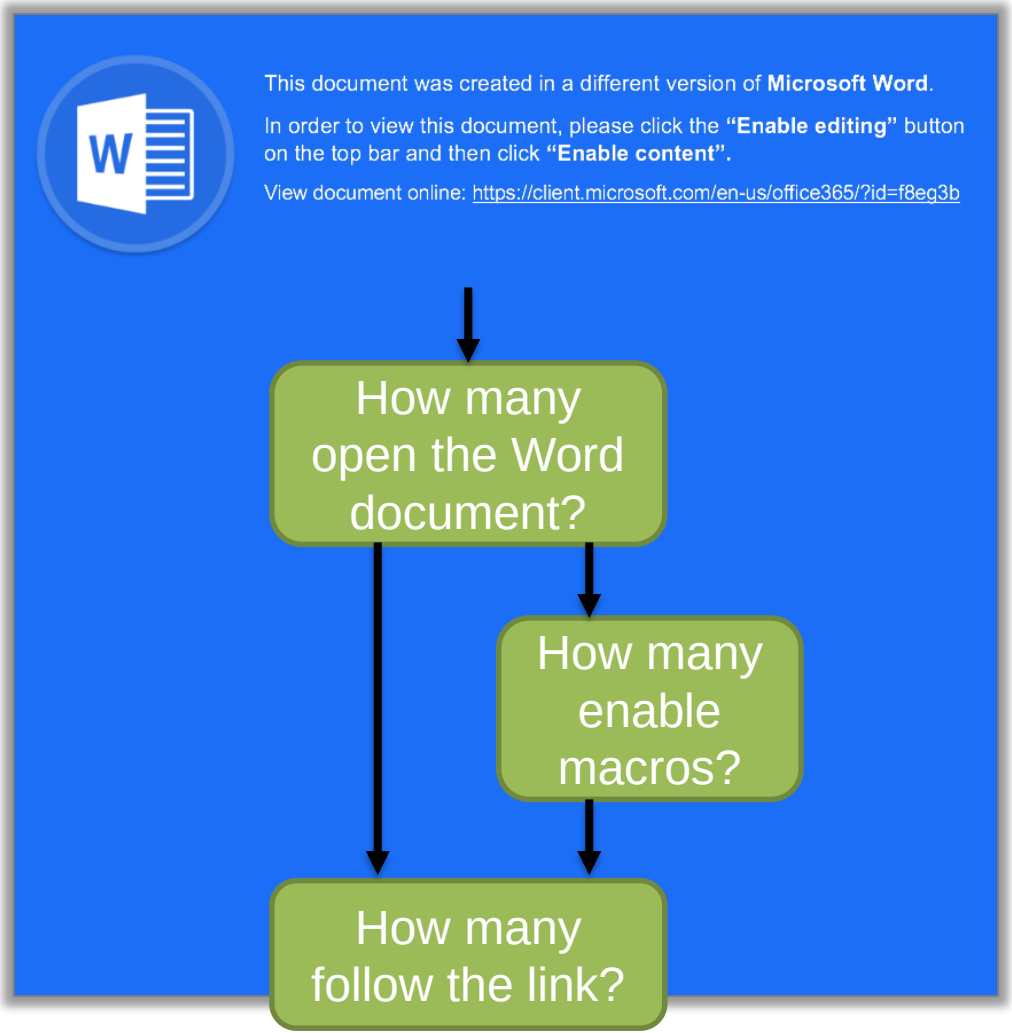
To: [redacted]

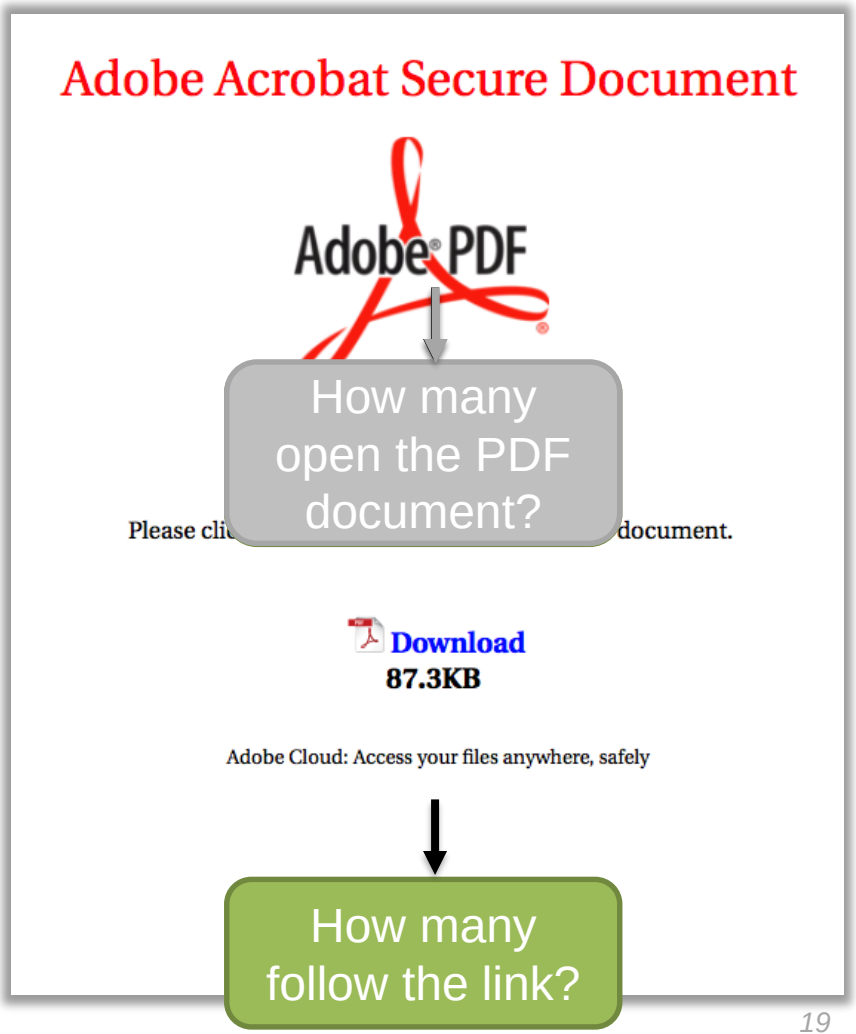
Dear [redacted]

Please see the attached for report on pension fund balance situation.

Regards
Federico Campesi
Finance Management

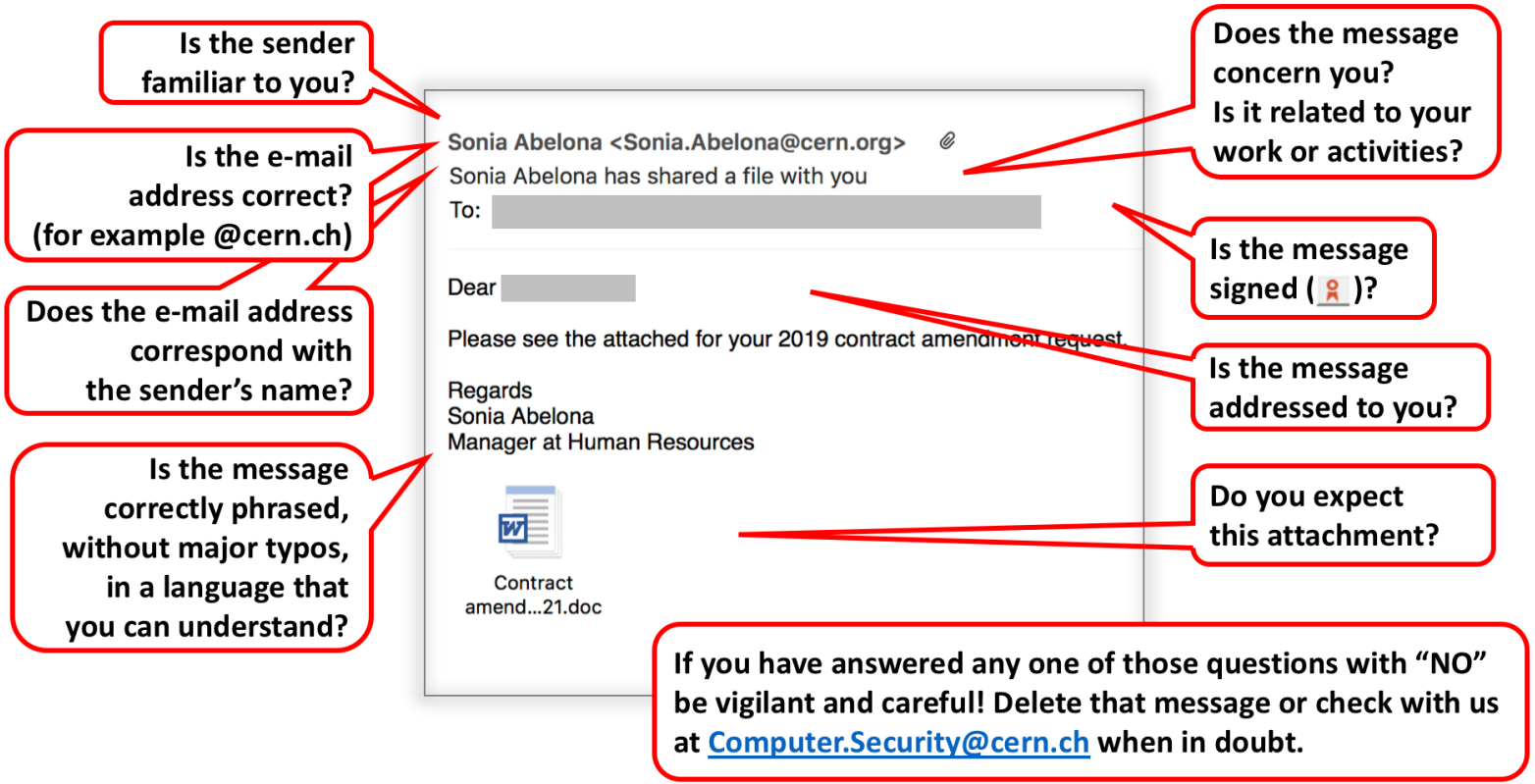
Fund balance - confidential.pdf

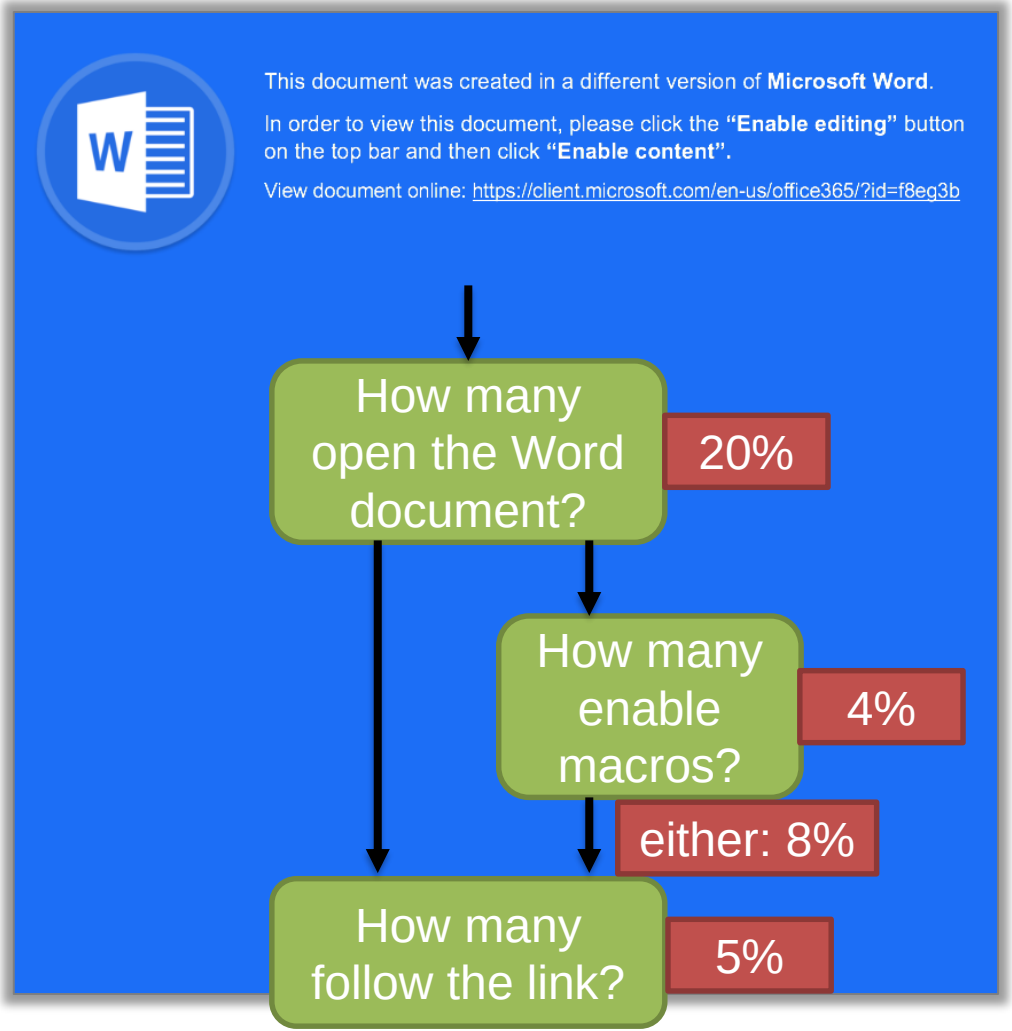

This document was created in a different version of Microsoft Word.
In order to view this document, please click the "Enable editing" button on the top bar and then click "Enable content".
View document online: https://client.microsoft.com/en-us/office365/?id=f8eg3b
How many open the Word document?
How many enable macros?
How many follow the link?

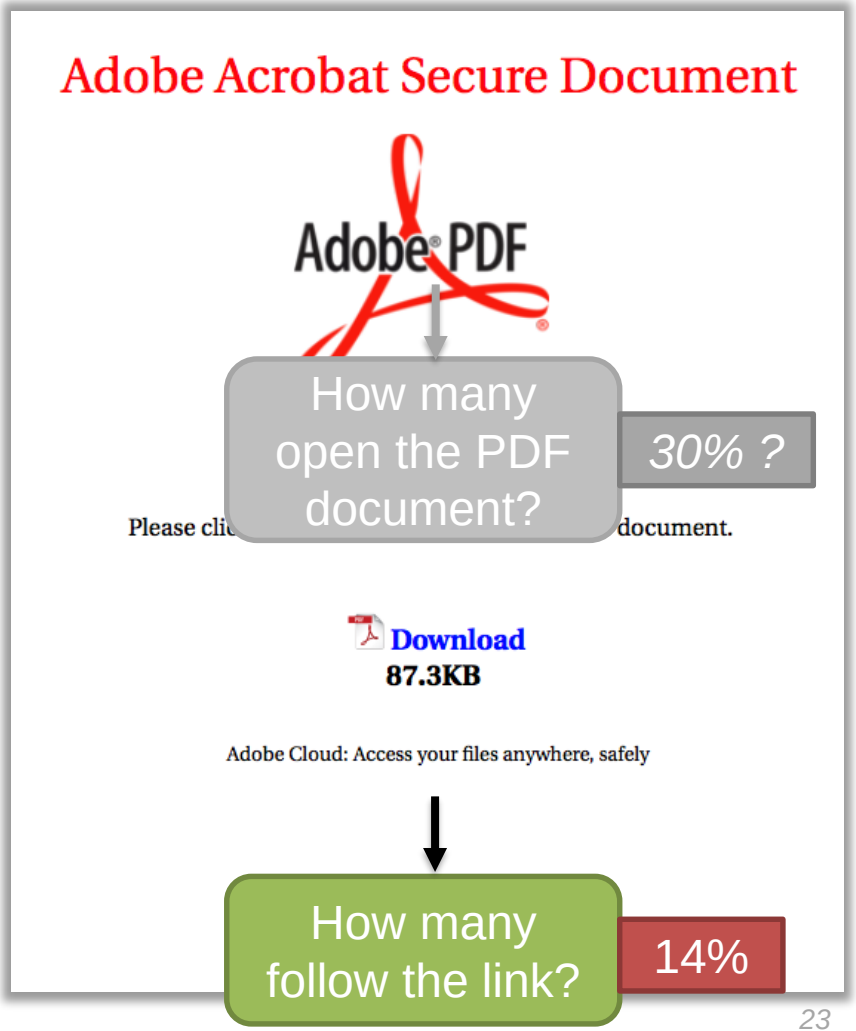

Adobe Acrobat Secure Document
Adobe PDF
How many open the PDF document?
document.
Download
87.3KB
Adobe Cloud: Access your files anywhere, safely
How many follow the link?

If you click on the link, you get redirected to [this page]:

... with hints on **how to identify malicious emails**:




This document was created in a different version of Microsoft Word.
In order to view this document, please click the "Enable editing" button on the top bar and then click "Enable content".
View document online: https://client.microsoft.com/en-us/office365/?id=f8eg3b
How many open the Word document?
20%
How many enable macros?
4%
either: 8%
How many follow the link?
5%


Adobe Acrobat Secure Document
Adobe PDF
How many open the PDF document?
30% ?
document.
Download
87.3KB
Adobe Cloud: Access your files anywhere, safely
How many follow the link?
14%

What works?

Please see the attached *for report on pension fund balance situation.* 18%
for your 2019 contract amendment request. 24%
with the confidential design report. 15%
on your input to our results. 17%
on new IT security measures. 15%

HEPiX Fall 2015 campaign:
*Get a voucher for **free drinks***

From @cern.com 17%
@cern.org 17%
@cem.ch 18%
@cerm.ch 16%
@cern.ch 20%

Dear sebastian 18%
Dear Sebastian 18%

People respond

- ***I am unable to contact Ralf Brant*** *(or Brandt!).* ***He is not in the CERN phonebook****. Please help. I am trying to send some info.*
- *I received this mail, as* ***coming from a cern address and headed to me, I trusted it and opened the pdf***
- *I have received this Email,* ***I am unable to open the attachment and I am starting to worry that it is not from CERN.***
- ***I have opened the attachment****, I noticed that the sender address is incorrect (@cerm.ch) ,* ***I'm confused a bit ... is it an malicious emails !?*** *if yes , what should i do !?*
- *The email was* ***directed at me with some accurate details.***
- *The attached file is strange (I could not open it)*
- *Today morning I was opening my e-mails, as I had much feedback, I've received documentation that I was waiting for.* ***Meanwhile, I got an e-mail improper, but I was not awake enough and I've opened it.***
- ***Since the email address is a CERN address, I thought it's no problem****, I downloaded the attachment and tried to open it. However, I cannot open it neither on Linux nor on Windows. I tried to reply to this address but I always get rejected (delivery failure)*

People respond

- *A design report of only 35 kB file size sounds suspicious.*
- *I am **a summer student who just recently arrived** at CERN. Today I received a weird email [..] **I opened it. Now I realise how silly that was***
- *as always **I detected this mail as the regular test from IT security. I really enjoy them,** because they are quite well designed and lead to a very informative site about mail scams and how to detect them.*
- *Could you please explain what is going on? I believe **you are violating CERN's code of conduct...***

Commercial solutions,
open-source tools

Commercial solutions: simulated phishing campaigns

- Engagement, gamification
- Classroom courses → **continuous micro-training in work environment**
- Security awareness → **behavior change**

- Examples: HOXHUNT PHISHLABS phishing box KnowBe4 Human error. Conquered.
  - every user receives ~3 messages per month (apparently deemed acceptable)
  - growing difficulty of messages, increasing level of "truth",
    using internal information e.g. names of executives or projects
  - users report malicious mails with a button in Outlook → feeding the SOC

Is simulated phishing worth the effort? **Yes**

Should failing phish tests be a fireable offense? **No**

Open-source tools also available

SocialFish

BLACKEYE

Conclusions

People and technology
… an unsolvable problem?

"I received this mail, as coming from a cern address and headed to me, ***I trusted it*** *and opened the pdf"*