

Tricking your users: simulated phishing campaigns at CERN

Sebastian Łopieński

CERN Deputy Computer Security Officer



HEPiX Autumn 2020

13 October 2020

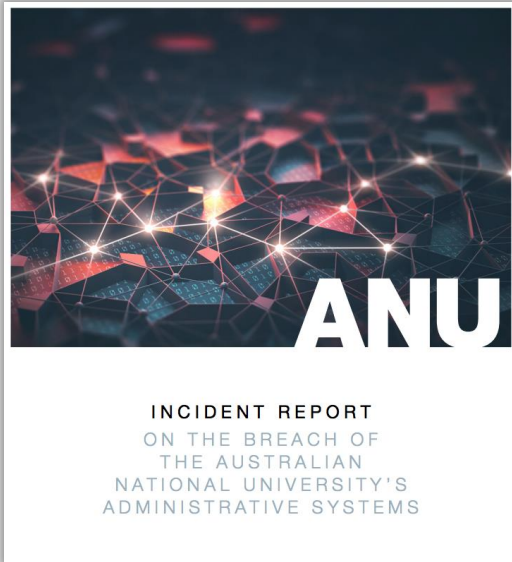
Instead of “why”: the 2019 data breach at ANU

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”*

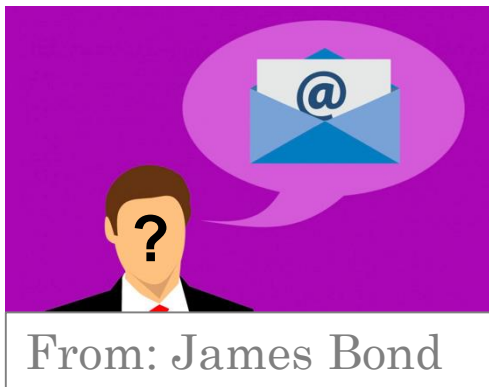


E-mail is the main attack vector



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



Not only phishing.

- Password fishing (“phishing”)
- Malware infections
 - ransomware, APT etc.
- Regular fraud, extortion etc.
 - *“Hi, I am in trouble, can you help?”*
 - *“Dear Sir, you are under investigation...”*
- CEO fraud
- Business email compromise
 - *“Here is our new bank account number”*

Not only email.

- Email
- SMS, WhatsApp etc.
- Phone calls
- New platforms for videoconferencing and online collaborations

**Everyone teleworking?
Whole new opportunities!**

Technical protection measures exist...

...however, humans are the first *and* last line of defense

Simulated phishing campaigns

hepix2015@bnl.gov <hepix2015@bnl.gov>

5-security

10 October 2015 at 19:00

H

HEPiX workshop - welcome, registration, free drinks offer

To: hepix2015@bnl.gov <hepix2015@bnl.gov>

Dear HEPiX Fall 2015 participants,

With our workshop starting this Monday, we are excited and looking forward to welcoming you at BNL very soon.

As a reminder, the registration takes place 8-9am, and we start with the first presentation already at 9am - please be on time.

<https://indico.cern.ch/event/384358/timetable/>

I'm happy to announce that we managed to negotiate free drinks offers with several of the suggested restaurants. The voucher code to be used is "hepix2015". For more details and for obtaining one of the limited number of vouchers, please see here:

<https://indico.cern.ch/event/384358/page/4209-restaurant-vouchers>

Wish you all a safe travel!

Best regards,
Tony Wong
for the Local Organizing Committee

<http://voucher.x10host.com/?coupon=hepix2015&q=10ad0>

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)
“phishing” website
(2020)

Various messages, senders, sender domain etc.

Sonia Abelona <Sonia.Abelona@cern.org> 

Sonia Abelona has shared a file with you

To: 

Dear 

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: 

Dear 

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

Regards

Federico Campesi
Finance Management



Fund balance -
confidential.pdf

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



The banner features the CERN logo on the left, followed by the text "CERN Computer Security". On the right, a red rounded rectangle contains the text "Computer security emergency contact", the email address "Computer.Security@cern.ch" with a phone icon and "70500", and the French translation "Contact en cas d'incident de sécurité informatique". The background of the banner is a blue-tinted image of binary code (0s and 1s) with a bright light source shining through a keyhole in the center.



(Version française en-dessous)

Oops... The email and the attachment you have just opened are fake, and potentially malicious!

You just fell for a scam. The attached document that you have opened is fake, and potentially malicious. Your "click" could have had severe operational and financial consequences for CERN... Let us explain to you how you can better identify malicious emails and attachments, and what consequences opening them might have for you and your digital assets...

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

The image shows a screenshot of an email interface with several red callout boxes containing questions. The email content is as follows:

From: Sonia Abelona <Sonia.Abelona@cern.org> [Profile icon]

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

Attachment: Contract amend...21.doc

Callout questions:

- Is the sender familiar to you?
- Is the e-mail address correct? (for example @cern.ch)
- Does the e-mail address correspond with the sender's name?
- Is the message correctly phrased, without major typos, in a language that you can understand?
- Does the message concern you? Is it related to your work or activities?
- Is the message signed (👤)?
- Is the message addressed to you?
- Do you expect this attachment?

Summary box: If you have answered any one of those questions with "NO" be vigilant and careful! Delete that message or check with us at Computer.Security@cern.ch when in doubt.

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

Dear colleague,

Please see here for your 2020 contract amendment request:

<https://hr.cern.ch/76342518/Contract%20amendment%2039421>

Regards

Anne Darenport-Smid

Manager at Human Resources

http://192.91.245.24/hr.cern.ch/76342518/
Contract%20amendment%2039421?
u=c0a-20eb2008&c=hr-drcc-lcu&a=t



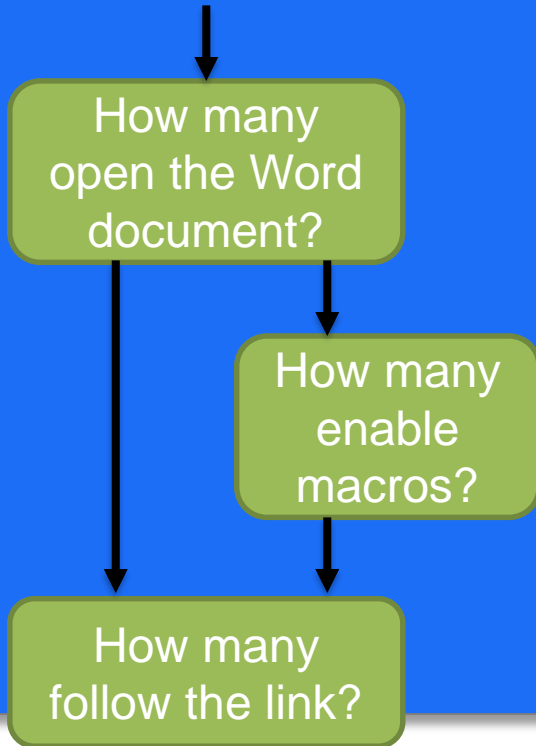
192.91.245.24/documentstore.cern.ch/?u=c0a



http://hr.cern.org/files/37543811.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>



Adobe Acrobat Secure Document



How many open the PDF document?

Please click [here](#) to open the document.

 **Download**
87.3KB

Adobe Cloud: Access your files anywhere, safely

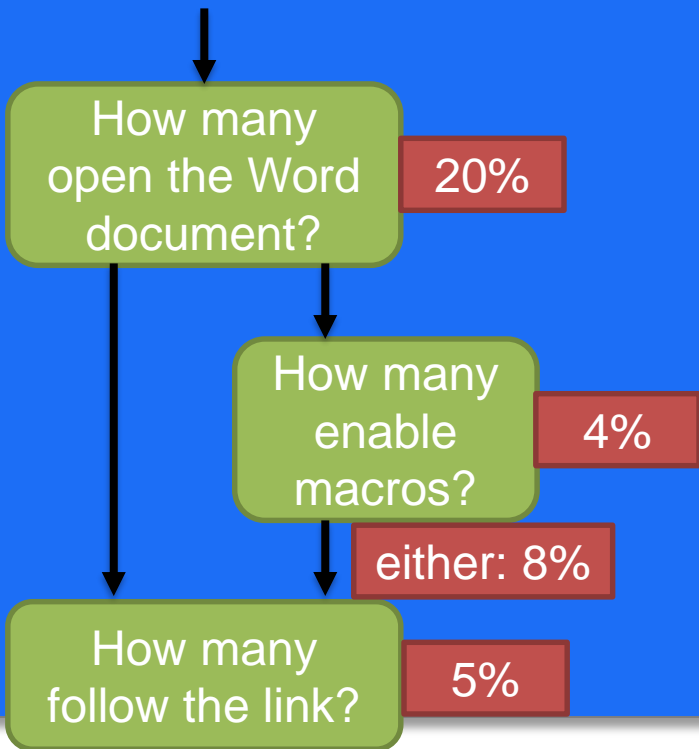
How many follow the link?



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>



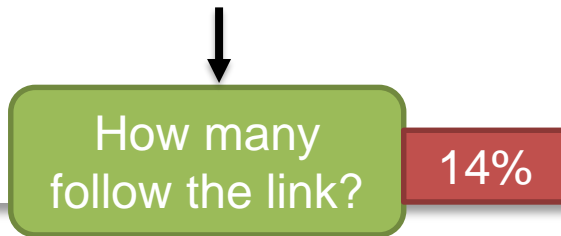
Adobe Acrobat Secure Document



Please click document.



Adobe Cloud: Access your files anywhere, safely



Password field disabled

Some users try several times

CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

Sign in with your CERN account

Reminder: you have agreed to comply with the CERN computing rules, in particular OC5. CERN implements the measures necessary to ensure compliance.

Use credentials

Username or Email address Password Sign in

Remember Username or Email Address [Need password help ?](#)

Use one-click authentication

- Sign in using your current Windows/Kerberos credentials [autologon] Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC (Firefox help here).
- Sign in using your CERN Certificate [autologon] You can get a CERN certificate on the CERN Certification Authority website.

Use strong two factor authentication [show]

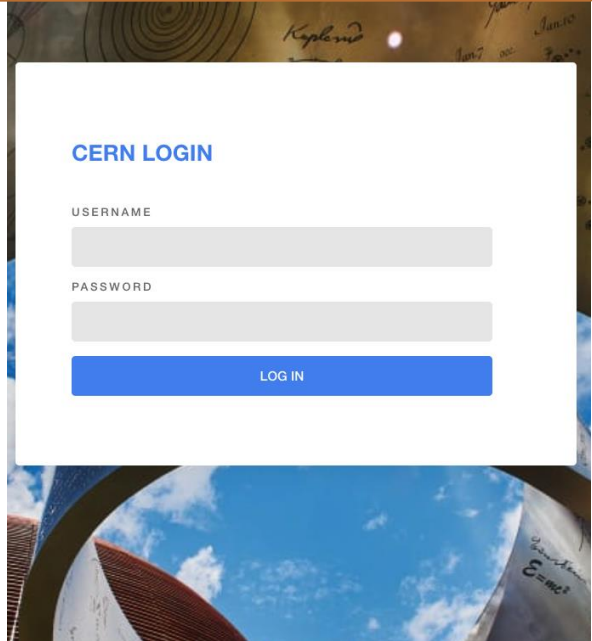
Sign in with a public service account

Facebook, Google, Live, etc. Authenticate using an external account provider such as Facebook, Google, Live, Yahoo, Orange.

Sign in with your organization or institution account

eduGAIN Enter the name of the organisation you are affiliated with... Go Why is my organisation not listed?

Log in with your CERN account Username Password Forgot Password? Log In Reminder: you have agreed to comply with the CERN Computing Rules, in particular OC5. CERN implements the measures necessary to ensure compliance.



“Real” existing SSO

9.8%

“Real” new SSO

10.7%

Non-existing SSO

9.4%

What worked in 2020? (phished rates)

your 2020 contract amendment request

15%

pension fund balance situation

8%

confidential covid-19 report

9%

new teleworking rules

7%

DOC attachment

7%

PDF attachment

7%

documentstore.cern.ch link

13%

Topic-specific link

12%

Dear colleague

9%

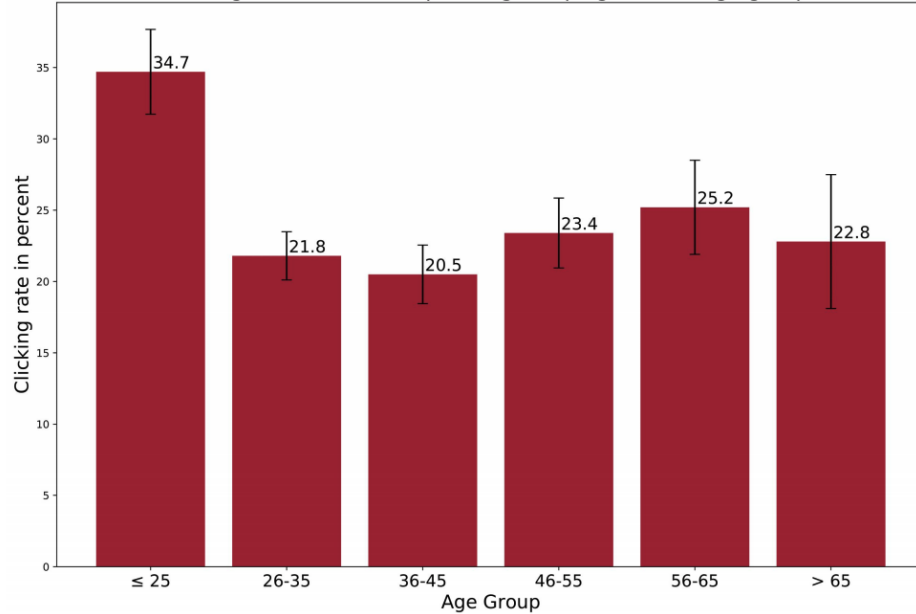
Dear Sebastian

11%

But who clicks?

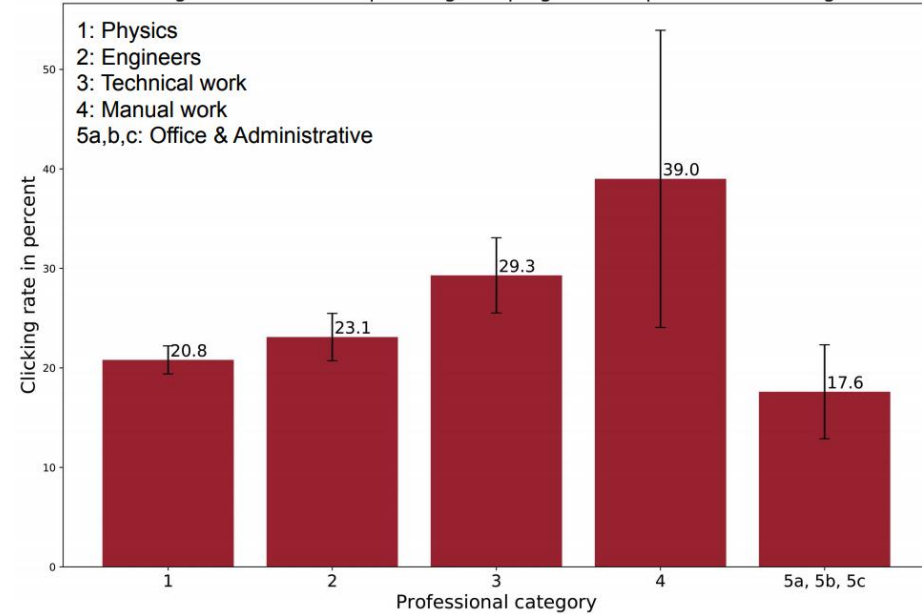
(2019 results - [analysis](#) by T.Betz)

Clicking rate of the 2019 phishing campaign across age groups



Young people have lower (financial) risk aversion?

Clicking rate of the 2019 phishing campaign across professional categories



NB: no difference between genders

We are not the only ones

GitLab



Laptop Refresh Program

Congratulations. Your IT Department has identified you as a candidate for Apple's System Refresh Program. The following Macbook Pro has been selected for you:

MacBook Pro (15-inch, 2019)
2.4 GHz 8-Core Intel Core i9
16GB Memory

To customize your laptop or to learn more about the program please [click here and sign into GitLab.](#)

Regards,
Apple

For help with subscriptions and purchases, visit [Apple Support.](#)

20% phished

Copyright © 2020 Apple Inc.
[All rights reserved](#)

Tribune Publishing

We are pleased to inform you that we are providing targeted bonuses between 5,000 and 10,000 dollars this year. Tribune Publishing is able to provide this bonus as a direct result of the success created by the ongoing efforts to cut our costs!



Caroline Glenn @bycarolineglenn · Sep 23

Most of our staff are underpaid to begin with. Some are struggling mentally and financially to keep working through this pandemic. Some have gotten sick with Covid.

To dangle a phony bonus to see who will fall for a phishing email is downright cruel and unimaginably tone deaf.

You will need to login below to view your end of year
ele
into

Big backlash, public criticism
Company apologized

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”*

BACKUP SLIDES

What worked in 2019?

(click rates)

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

From @cern.com

17%

@cern.org

17%

@cem.ch

18%

@cerm.ch

16%

@cern.ch

20%

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

Dear sebastian

18%

Dear Sebastian

18%

18%

24%

15%





17%

15%

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:    
 - 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

What we have seen at CERN

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

10.12.2018, 20:37, [REDACTED]

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

Subject: Giovanni [REDACTED] has shared a

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

Hi [REDACTED],

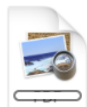
This is safe and secured to access

Get back to me soon as you get this .

Regards
Giovanni [REDACTED]

Please see the attached for your action

Regards
Giovanni [REDACTED]



Scan.pdf


Scan (1).pdf - Adobe Reader

File Edit View Window Help

Open | [Icons] | 1 / 1 | 105% | [Icons] | 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](#)

► 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.

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](#)

Sign In

Export PDF

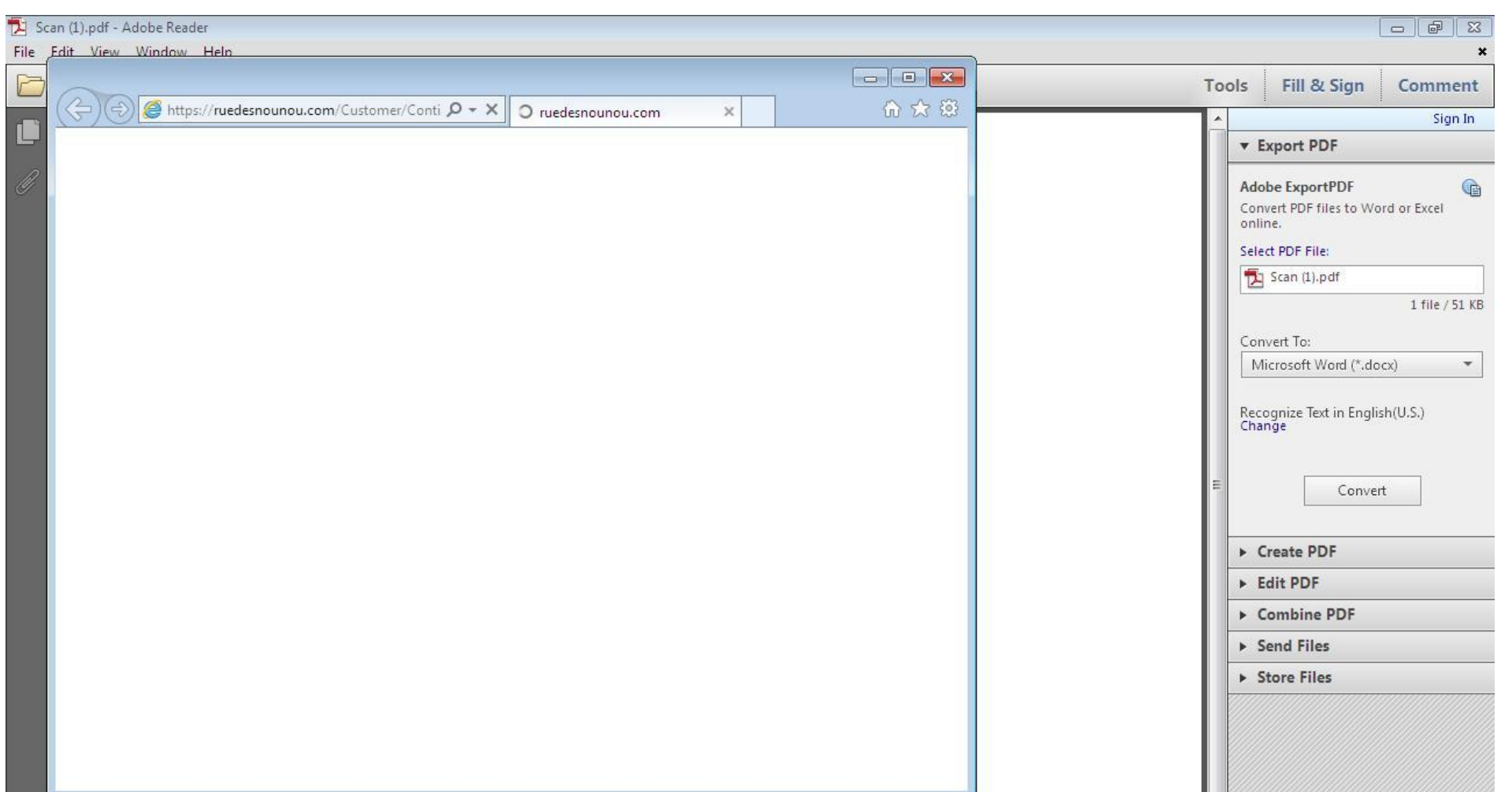
Adobe ExportPDF
Convert PDF files to Word or Excel online.

Select PDF File:
 1 file / 51 KB

Convert To:

Recognize Text in English(U.S.)
[Change](#)

► Create PDF
► Edit PDF
► Combine PDF
► Send Files
► Store Files



F

FILE HOME INSERT DATA REVIEW VIEW Tell me what you want to do OPEN IN EXCEL

Clipboard: Undo, Paste, Cut, Copy

Font: Calibri, 11, Bold, Italic, Underline, Text Color, Background Color, Font Color

Alignment: Wrap Text, Merge & Center

Number: ABC 123, Number Format

Tables: Survey, Format as Table

Cells: Insert, Delete

Editing: AutoSum, Clear, Sort, Find

fx

	A	B	C	D	E	F	N	O	P	Q	R	S	T	U
1		PAGE 1/40												
2														
3														
4														
5														
6						(1) CONTRACT TERMS AND CONDITION / CE								
7														
8														
9														
10						(2) FUND ALLOCATION / PURCHASE ORDER (
11														
12														
13														
14						(3) DELIVERY PERIOD (duration) / PORT OF DESTINATION								
15														
16														
17														
18						(4) DELIVERY TERMS / PAYMENT TERMS / QUOTE VALIDITY								

Office Excel

someone@example.com

Password

Download

Starting...

CONFIDENTIAL DOCUMENT

... 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 [REDACTED] <lindajeff99@aol.com>

Junk - CERN Yesterday at 17:13

URGENT

To: [REDACTED] <[REDACTED]@cern.ch>

[REDACTED]
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 [REDACTED]

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

Technical protection measures do help

During the campaign:

- **Macros** in downloaded documents (e.g. received via e-mail) are **blocked** on all CERN Windows machines
- CERN **anti-virus started detecting** these attachments

Afterwards:

- CERN user uploaded a sample to VirusTotal, vendors picked up
 - because the filename included word “confidential”
- DOC attachment detected by AV products as [Win32/Skeeyah.A!rfn](#) trojan

