

Cybercriminels *contre* vous et moi

Que risquons-nous en ligne et comment s'en protéger

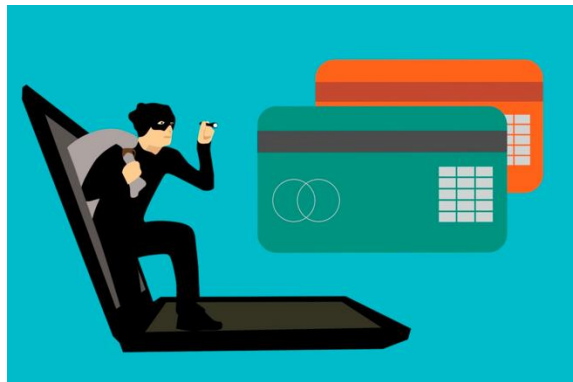
Présenté par
l'équipe de sécurité informatique du CERN



CERN Open Days 2019
14-15 September



Comment les cybercriminels se font de l'argent ?



Trojans de banque en ligne



Hameçonnage



Usurpation d'identité



Rançons



Extorsion et arnaques



Crypto-monnaies (minage)

Les **courriels** sont le principal vecteur d'attaque

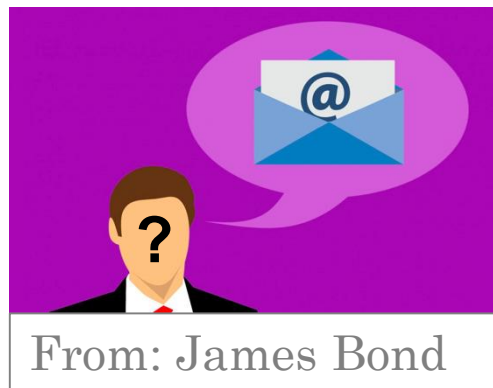


Les courriels sont le principal vecteur d'attaque

Envoyer des courriels est **très simple et pas cher**



Fausser l'expéditeur d'un courriel est trivial



Les courriels malicieux contiennent des **pièces jointes infectées** et **liens** vers des sites malicieux



Voyons quelques tactiques courantes
de criminels

Exemple 1

Comment duper une victime
(sans même infecter son ordinateur)

(*) En réalité, l'ordinateur n'est pas infecté et il n'y a aucun enregistrement

(*) En réalité, l'ordinateur n'est pas infecté et il n'y a aucun enregistrement

Hello!

Truc 1: Envoyer le courriel “depuis” le compte de la victime

If you want to prevent this, transfer the amount of \$500 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

Demander de l'argent (crypto-monnaie)

It is just so unfortunate. I am aware [REDACTED] is your password. Moreover, I know your secret and I have evidence of your secret. You do not know me and no one hired me to check out you.

Truc 2: Utiliser un mot de passe fuité

Exemple 2

Comment voler le mot de passe d'une victime
et prendre contrôle de ses comptes en ligne

Hameçonnage classique

● Mail Delivery System <[redacted]@cern.ch>

24 July 2019 at 08:36

MS

Message Delivery Status Notification (Failure)

To: [redacted]@cern.ch

Hello [redacted]
[redacted]@cern.ch

Your messages are now returning a failure delivery because your email has not been verified, you are required to confirm your email account to restore normal email delivery.

This helps us stop automated programs from sending you spam.

[Confirm \[redacted\]@cern.ch](#)

Please note
• Log in
man
Once Verified
Sincerely,
cern mail delivery system

<https://microsoftof7ahw99n6twblh.z13.web.core.windows.net/index.php?c=eee010ae0e015ae0e014ae05ae0.e08ae0e016ae019ae4e011ae014ae02ae0e08ae1ee01ae1e013ae010ae01ae05a>

2 Hours

Lien malicieux

Lien légitime

This is a mandatory service communication for [redacted]@cern.ch.

This message was sent from an unmonitored e-mail address. Please do not reply to this message.

[Privacy](#) | [Legal](#)

<http://click.email.microsoftonline.com/?qs=d306d1daab078722535d35b5ecac1aba5f08f80731a1b3192b6b6d6198c35cc9d4370eaec2bd374e44641c036f61e2c5>

Exemple 3

Comment infecter l'ordinateur d'une victime
et voler ses mots de passe

From: Giovanni [REDACTED] <office.outlook@[REDACTED]>
Date: Monday, 10 December 2018 at 10:37
To: [REDACTED]
Cc: [REDACTED]

10.12.2018, 20:37, [REDACTED]

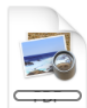
Dear Giovanni,
I think this might be fishing !
Can you confirm ?
Thanks,
[REDACTED]

Subject: Giovanni [REDACTED] has shared a [REDACTED]

Please see the attached for your action

Regards

Giovanni [REDACTED]



Scan.pdf

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 [Icons] 1 / 1 [Icons] 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](#)

Convert

► Create PDF


► Edit PDF

► Combine PDF

► Send Files

► Store Files

Adobe Acrobat Secured Document

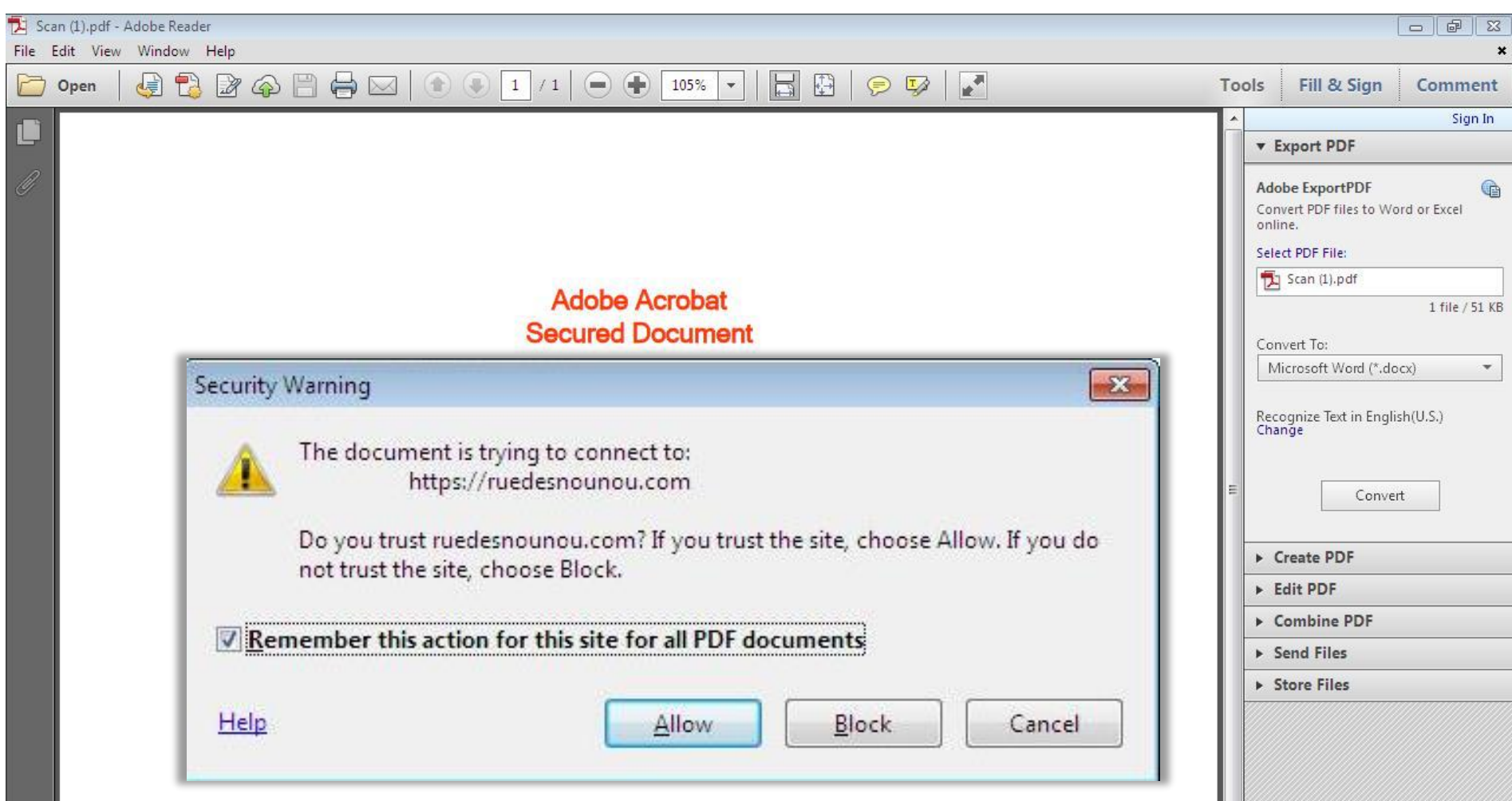


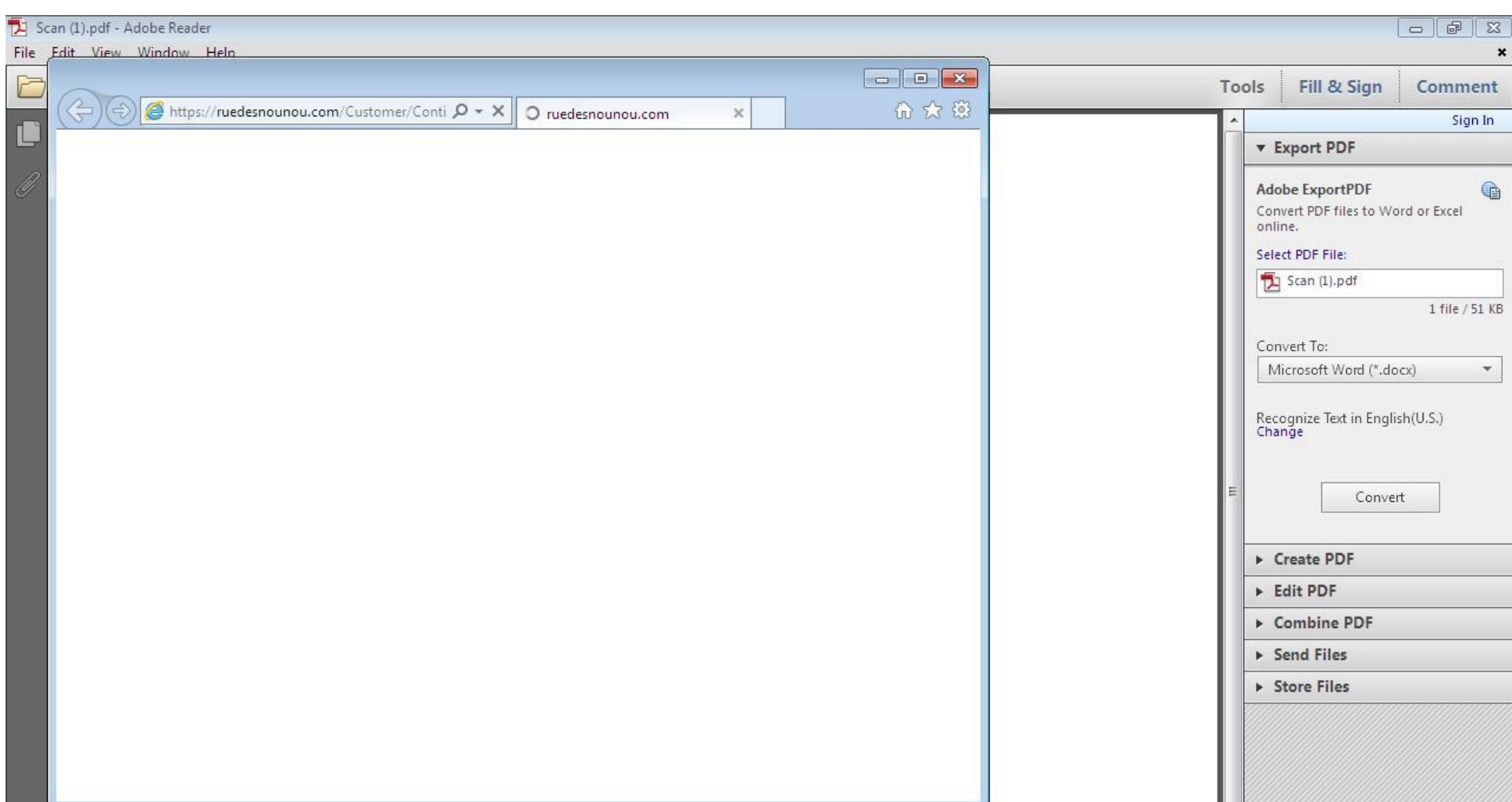
Adobe Acrobat
PDFXML Document

Click on Download Adobe Document below
&
verify your email / login to securely access files!

[Download Document](#)
Size: 88.7 KB

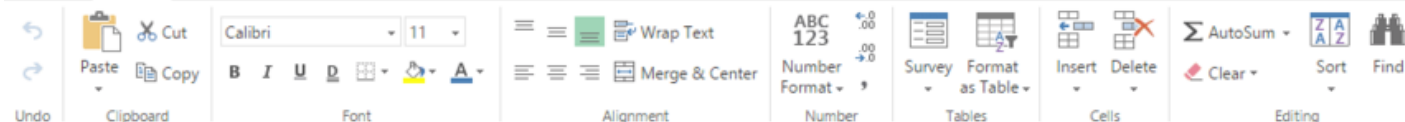
Adobe Cloud: Have all your files within reach from any device.





F

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



fx

	A	B	C	D	E	F	N	O	P	Q	R	S	T	U
1		PAGE 1/40												
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														

... six mois plus tard ...

● Giovanni [redacted] <angelavidos340@gmail.com>

19 June 2019 at 12:33

Respond

To: [redacted]@cern.ch>



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

Bonus

Techniques avancées

Techniques plus avancées utilisées par des criminels

- **Harponnage** : hameçonnage ciblant une personne précise
 - Fabriqué en utilisant des informations collectées à l'avance: noms de projets, de collègues, hiérarchie, qui est absent, etc.
 - Envoyé « depuis » un collègue, un partenaire ou même votre patron
- **Utilisez le carnet d'adresse** : Après avoir compromis une boîte mail, envoyer des courriels « depuis » la victime à ses contacts
- **S'ajouter à une conversation** : Après avoir compromis une boîte mail, répondre à une conversation existante en rajoutant un contenu malicieux

Comment se défendre ?

Défense – règles d'or

Règle 1: ne faites pas confiance aux courriels

- *L'expéditeur peut être faux* – tous le monde peut être president@gouv.fr
- Ne cliquez pas sur les liens venant de courriels suspects
 - En cas de doute, tapez à la main le lien dans votre navigateur
- N'ouvrez aucune pièce jointe inattendue, n'activez pas les « macros »

Règle 2: ne soyez pas victime d'arnaque et d'hameçonnage

- Non, vous n'avez pas gagné, hérité d'une fortune ou reçu une affaire d'enfer
- Non, votre banque / Paypal / ... ne vous demande pas de confirmer votre compte
- Non, votre patron ne vous demande pas secrètement de faire un transfert spécial
- Non, le support technique ne vous contacte pas pour vous aider

Défense – règles d'or

Règle 3: **Soyez prudents sur Internet**

- Réfléchissez avant de cliquer
- Assurez-vous que vous êtes *vraiment* sur le bon site
- N'installez pas de logiciels non fiables téléchargés sur Internet

Règle 4: **Protégez votre ordinateur**

- Maintenez votre système d'exploitation (Windows, Mac OS etc.) à jour
- Maintenez vos logiciels à jour (surtout votre navigateur et ses extensions)
- Utilisez un anti-virus, maintenez le à jour

Règle 5: **Protégez vos mots de passe et comptes en ligne**

- Utilisez des mots de passe forts, et utilisez des gestionnaires de mots de passe
- Ne réutilisez pas vos mots de passe (même mot de passe sur plusieurs sites)
- Activez l'authentification forte (multi-facteurs) dès que possible

Les êtres humains et la technologie

... un problème insoluble?

