

COMMUNICATION DU PMO

Alerte à l'escroquerie téléphonique!

Madame, Monsieur,

Nous souhaitons attirer votre attention sur des escroqueries **téléphoniques** visant des pensionnés des institutions européennes.

Des escrocs appellent les pensionnés pour leur 'proposer' une 'aide sociale' supplémentaire de 500 euros ou plus. La première question qu'ils pourraient poser est : "Êtes-vous vacciné ?". Ensuite, ils demandent le numéro personnel et autres données personnelles, telles que numéros de comptes bancaires et mots de passe.

De telles demandes faites par téléphone ou par e-mail ne proviendront jamais du PMO ou de la Commission européenne ! Nous utilisons nos applications et plateformes sécurisées, telles que RCAM en ligne, EU Login et FiLIP pour obtenir et vérifier les informations dont nous avons besoin afin de gérer vos dossiers, questions et demandes.

Nous ne vous demanderons jamais:

- **de communiquer des données personnelles ou des informations sur votre compte bancaire par téléphone ;**
- **de partager des codes pin et des mots de passe ;**
- **d'effectuer des transactions bancaires.**

Méfiez-vous de toute personne qui vous demande de telles données et actions - il s'agit certainement d'escrocs qui tentent de vider votre compte bancaire !

Soyez vigilant(e) et ne communiquez jamais vos mots de passe, codes pin ou autres informations personnelles sensibles !

XXXXXXXXXXXXXXXXXXXX

COMMUNICATION FROM PMO

Scam alert: phone frauds!

Dear Madam,

Dear Sir,

We wish to draw your attention to **phone frauds** targeting pensioners from the EU institutions.

Scammers call pensioners 'offering' additional 'allowance' of 500 euros or more. Among the first questions they ask could be: 'Are you vaccinated?' Then they ask for the personal number and other personal details, such as bank accounts and passwords.

Such questions and requests over the phone or via e-mail would never come from the PMO or the European Commission! We use our secured applications and platforms, such as EU Login, JSIS and FiLIP to collect and verify the information we need to process your files, questions and requests.

We would also never ask you:

- **to give personal data or bank account information over the phone** or via e-mail;
- **to share pin codes and passwords;**
- **to carry out any bank transactions.**

Beware of anyone who asks for such data and actions - they can be only scammers trying to empty your bank account!

Please stay vigilant: it is never a good idea to give out passwords, pin codes and other sensitive personal information!

XXXXXXXXXXXXXXXXXXXX

MITTEILUNG VOM PMO

Warnung vor Telefonbetrug!

Sehr geehrte Damen und Herren!

Wir möchten Sie auf Telefonbetrügereien aufmerksam machen, die sich gegen Rentner der EU-Institutionen richten.

Betrüger rufen Rentner an, um ihnen eine zusätzliche "Sozialhilfe" in Höhe von 500 Euro oder mehr "anzubieten". Die erste Frage, die sie stellen könnten, lautet: "Sind Sie geimpft?". Danach fragen sie nach der Personalnummer und anderen persönlichen Daten, wie Bankkontonummern und Passwörtern.

Solche Anfragen, die per Telefon oder E-Mail gestellt werden, werden niemals vom PMO oder der Europäischen Kommission stammen! Wir verwenden unsere sicheren Anwendungen und Plattformen wie GKFS Online, EU Login und FiLIP, um die Informationen zu erhalten und zu überprüfen, die wir benötigen, um Ihre Fälle, Fragen und Anträge zu bearbeiten.

Wir werden Sie niemals darum bitten:

- **persönliche Daten oder Informationen über Ihr Bankkonto per Telefon weiterzugeben;**
- **Pin-codes und Passwörter weiterzugeben;**
- **Bankgeschäfte zu tätigen.**

Seien Sie misstrauisch gegenüber Personen, die Sie um solche Daten und Handlungen bitten - es handelt sich dabei mit Sicherheit um Betrüger, die versuchen, Ihr Bankkonto zu leeren!
Seien Sie wachsam und geben Sie niemals Ihre Passwörter, Pin-Codes oder andere sensible persönliche Informationen weiter!

We have been informed that swindlers are using a new phishing technique. The person on the phone says that she is calling from the European Commission Pension Unit. She says that the European Commission wants to pay a Covid-19 premium of 800 € because of the average pension of the pensioner in question (how do they know?).

When asked why the Commission did not send out an e-mail about this, the reply is that the pension service (sic) decided to call people. (they never do!)

Then the person on the phone asks to verify one's bank account details. The answer to this is that if that person is really calling from the Pension Unit of the European Commission, she should have the bank account details. At that stage the person usually becomes rude, says you are naive and puts down the telephone.

But how did the swindler get the telephone number of a pensioner in the first place??

XXXXXXXXXX

Nous avons été informés que les escrocs utilisent une nouvelle technique d'hameçonnage (phishing). La personne au téléphone dit qu'elle appelle de la part de l'Unité Pensions de la Commission européenne. Elle dit que la Commission européenne veut payer une prime Covid-19 de 800 € en raison de la pension moyenne du retraité en question (comment le savent-ils ?).

A la question de savoir pourquoi la Commission n'a pas envoyé un e-mail à ce sujet, la réponse est que le service (sic) des pensions a décidé d'appeler les gens. (ils ne le font jamais !)

Ensuite, la personne au téléphone demande de vérifier les coordonnées du compte bancaire. La réponse est que si cette personne appelle vraiment de l'Unité Pensions de la Commission européenne, elle devrait avoir les détails du compte bancaire. À ce stade, la personne devient généralement impolie, dit que vous êtes naïf et raccroche le téléphone.

Mais comment ces escrocs ont-ils pu obtenir le numéro de téléphone d'un retraité ?

XXXXXXXXXX

Wir wurden darüber informiert, dass Betrüger eine neue Phishing-Methode anwenden. Die Person am Telefon behauptet, sie rufe von der Rentenabteilung der Europäischen Kommission an. Sie sagt, die Europäische Kommission wegen der Durchschnittsrente des betreffenden Rentners (woher wissen sie das?) eine Covid-19-Prämie von 800 € auszahlen zu wollen.

Auf die Frage, warum die Kommission keine E-Mail dazu verschickt hat, antwortet sie, dass die Rentenstelle (sic!) beschlossen hat, die Leute anzurufen. (Das tun sie nie!)

Dann bittet die Person am Telefon darum, die Kontodaten zu überprüfen. Die Antwort darauf ist, dass die Bankverbindung vorliegen müsste, wenn die Person wirklich vom Referat

Renten der Europäischen Kommission anruft. Daraufhin wird die Person in der Regel unhöflich, sagt, Sie seien naiv und legt den Hörer auf.

Aber wie ist der Betrüger überhaupt an die Telefonnummer eines Rentners gekommen?



AIACE

Association Internationale des Anciens de l'Union européenne

Plus de 13.000 adhérents – ouverte aux anciens de toutes les institutions et tous les organes

Le Secrétaire Général



Bruxelles, le 30 septembre 2022

Objet : "fausses" invitations à renouveler le mot de passe RCAM

Le message du PMO n'étant pas à 100% clair, en voici un autre de l'AIACE qui met les choses au point de façon précise et concise.

Didier HESPEL

Attention à de "fausses" invitations à renouveler votre mot de passe RCAM !

(en complément du message du PMO diffusé précédemment et pour clarifier les choses)

En effet, des courriels malveillants sont envoyés par des escrocs prétendant représenter le RCAM. Veuillez ne jamais cliquer sur les liens de ces messages !

C'est uniquement votre mot de passe EU Login qui vous authentifie et permet de vous connecter à l'application "RCAM en ligne" (<https://webgate.ec.europa.eu/RCAM>) ou au menu "MyRemote" (<https://myremote.ec.europa.eu>) comprenant Sysper Post Activity, MyIntracomm, Staff Matters, Staff Contact. Ce mot de passe doit être modifié tous les 6 mois, mais ce changement de "password" vous sera toujours demandé lors d'une connexion et **jamais par email**.

Beware of "false" invitations to renew your JSIS password!

(addendum to the message from PMO previously circulated and to make things clear)

Indeed, malicious emails are being sent by scammers claiming to represent JSIS. Please never click on the links in these messages!

It is exclusively your EU Login password that authenticates you and allows you to connect to the "JSIS Online" application (<https://webgate.ec.europa.eu/RCAM>) or to the "MyRemote" menu (<https://myremote.ec.europa.eu>) including Sysper Post Activity, MyIntracomm, Staff Matters, Staff Contact. This password must be changed every 6 months, but you will always be asked to change your password when you log in and **never by email**.

15 Sections : Belgique/België – Danmark - Deutschland – Éire/Ireland - España - France – Ελλάς/Grèce - Italia – Luxembourg - Nederland – Österreich – Portugal – Suomi/Finland – Sverige - United Kingdom

Adresse administrative : Commission européenne, VM18 03/013, B-1049 Bruxelles

Téléphone : ligne directe (+32-2) 295.29.60 standard (+32-2) 299.11.11

Adresse électronique : aiace-int@ec.europa.eu Site Web: www.aiace-europa.eu

N° d'entreprise : 0408999411

Vorsicht vor "falschen" Aufforderungen, Ihr GKFS-Passwort zu erneuern!
(als Ergänzung zu der zuvor verbreiteten PMO-Nachricht und zur Klarstellung).

Tatsächlich werden bösartige E-Mails von Betrügern verschickt, die vorgeben, das GKFS (RCAM) zu vertreten. Bitte klicken Sie niemals auf die Links in diesen Nachrichten!
Es ist ausschliesslich Ihr EU Login-Passwort, das Sie authentifiziert und mit dem Sie sich in die Anwendung "RCAM Online" (<https://webgate.ec.europa.eu/RCAM>) oder in das Menü "MyRemote" (das Sysper Post Activity, MyIntracomm, Staff Matters, Staff Contact enthält; <https://myremote.ec.europa.eu>) einloggen können. Dieses Passwort muss alle 6 Monate geändert werden, aber diese Änderung des Passwortes wird immer beim Einloggen verlangt und **nie per E-Mail**.

15 Sections : Belgique/België – Danmark - Deutschland – Éire/Ireland - España - France – Ελλάς/Grèce - Italia – Luxembourg - Nederland – Österreich – Portugal – Suomi/Finland – Sverige - United Kingdom

Adresse administrative : Commission européenne, VM18 03/013, B-1049 Bruxelles
Téléphone : ligne directe (+32-2) 295.29.60 standard (+32-2) 299.11.11
Adresse électronique : aiace-int@ec.europa.eu Site Web: www.aiace-europa.eu
N° d'entreprise : 0408999411