**Passeport EDUCFI en voie professionnelle – Les arnaques**

**Niveaux d’études : CAP et seconde professionnelle**

* Visionner la vidéo "La minute cash" : Les arnaques – EDUCFI Banque de France
* Durée : 1’32
* Lien : <https://www.youtube.com/watch?v=5OACJ9dWWfQ>
* Lire et répondre aux questions suivantes.

1. Vous recevez le mail ci-dessous. Que faites-vous ?



* Je clique sur le lien et mets à jour mes données personnelles.
* Je contacte mon lycée pour l’informer de la réception de ce mail et lui demander ce que je dois faire.
* Je ne clique pas sur le lien et je supprime le mail.

1. ANTAI est l’agence nationale de traitement automatisé des infractions. Cette agence envoie notamment des textos pour signaler et rappeler les contraventions à régler. Vous recevez le texto ci-dessous. Deux éléments doivent vous alerter : c’est en effet un faux. Quels sont ces deux éléments ?



* ……………………………………………………………………………………………………….
* ……………………………………………………………………………………………………….

1. Vous achetez un objet sur un site de vente entre particuliers (Vinted, Leboncoin, Facebook Marketplace…). Le vendeur vous envoie un lien pour effectuer le paiement en ligne. Que faites-vous ?

* J’accepte le paiement en ligne et clique sur le lien.
* Je refuse ce paiement en ligne et je propose d’utiliser le système de paiement de la plateforme.

1. Un agent de ma banque m’appelle pour me demander des informations sur ma carte bancaire.

* Je lui communique les informations demandées.
* Je dis que je rappelle.

1. J’achète un livre sur un site d’e-commerce. Au moment de payer en ligne, on me demande de me connecter au site de ma banque pour confirmer le paiement. Que dois-je faire ?

* Je refuse et j’annule mon achat.
* Je suis rassuré et j’accepte cette authentification forte.

**Passeport EDUCFI en voie professionnelle – Les arnaques**

**Niveaux d’études : CAP et seconde professionnelle**

**CORRECTION**

* Visionner la vidéo "La minute cash" : Les arnaques – EDUCFI Banque de France
* Durée : 1’32
* Lien : <https://www.youtube.com/watch?v=5OACJ9dWWfQ>
* Lire et répondre aux questions suivantes.

1. Vous recevez le mail ci-dessous. Que faites-vous ?



* Je clique sur le lien et mets à jour mes données personnelles.
* Je contacte mon lycée pour l’informer de la réception de ce mail et lui demander ce que je dois faire.
* Je ne clique pas sur le lien et je supprime le mail.

1. ANTAI est l’agence nationale de traitement automatisé des infractions. Cette agence envoie notamment des textos pour signaler et rappeler les contraventions à régler. Vous recevez le texto ci-dessous. Deux éléments doivent vous alerter : c’est en effet un faux. Quels sont ces deux éléments ?



* L’État n’envoie pas de SMS à partir d’un téléphone (un numéro apparaît en effet dans l’entête du message).
* L’adresse du site est étrange. Elle doit se terminer par .gouv.fr. En cas de doute, il faut toujours vérifier : il est facile ici de saisir ANTAI dans un moteur de recherche et vérifier l’adresse, il y a même une page consacrée aux arnaques.

1. Vous achetez un objet sur un site de vente entre particuliers (Vinted, Leboncoin, Facebook Marketplace…). Le vendeur vous envoie un lien pour effectuer le paiement en ligne. Que faites-vous ?

* J’accepte le paiement en ligne et clique sur le lien.
* Je refuse ce paiement en ligne et je propose d’utiliser le système de paiement de la plateforme.

Sur les sites de vente en ligne entre particuliers, les paiements peuvent se faire soit en face à face, par exemple avec des espèces, soit via un système de paiement proposé directement par le site. Si le vendeur vous envoie un lien vers un autre dispositif en vous indiquant, par exemple, qu’il préfère cette solution, alors MÉFIANCE ! Le risque est réel qu’il vous redirige vers une autre plateforme ressemblant à un site légitime et qui récupère les données de votre carte bancaire.

1. Un agent de ma banque m’appelle pour me demander des informations sur ma carte bancaire.

* Je lui communique les informations demandées.
* Je dis que je rappelle.

Un banquier ne vous appellera jamais pour vous demander des informations sur vos moyens de paiement : c’est lui qui vous les a fournis, il les connaît parfaitement.

Dans ce genre de situation, l’appel vient toujours d’un escroc qui a récupéré votre numéro de téléphone et le nom de votre banque (vous avez peut-être été victime d’un faux site sur lequel vous avez renseigné ces informations).

Conseil : Raccrochez et, si vous avez un doute, rappelez votre conseiller au numéro de téléphone que vous connaissez pour clarifier la situation avec lui.

1. J’achète un livre sur un site d’e-commerce. Au moment de payer en ligne, on me demande de me connecter au site de ma banque pour confirmer le paiement. Que dois-je faire ?

* Je refuse et j’annule mon achat.
* Je suis rassuré et j’accepte cette authentification forte.

Les achats en ligne étaient auparavant confirmés avec un code reçu par SMS de la part de sa banque. Ce dispositif n’était pas suffisamment sécurisé pour lutter contre la fraude. Maintenant, chaque banque a mis en place un mécanisme d’authentification forte qui peut lui être propre appelé « clé digitale », « Certicode plus », « Sécuripass » ou encore « Pass sécurité ». Ce dispositif demande de confirmer le paiement directement sur l’application mobile de la banque. Il suffit de se connecter sur celle-ci grâce à votre code secret ou vos données biométriques (reconnaissance faciale, vocale ou empreintes digitales) pour que le paiement soit validé.

Pour les personnes ne disposant pas de smartphone ou qui ne pourraient pas utiliser l’application bancaire, d’autres solutions sont proposées par leur banque. Par exemple, la transaction peut être validée par l’envoi d’un SMS et complété par la saisie d’un code secret permanent. Certaines banques peuvent proposer à leurs clients des dispositifs électroniques générateurs de code à usage unique (token).