FFBRIDGE

Se protéger des arnaques en ligne

Les bons réflexes au quotidien, pour vous, pour vos proches et pour votre club



Webinar de sensibilisation proposé par la Fédération Française de Bridge

Les thèmes que nous allons parcourir ensemble

1. Pourquoi nous sommes tous concernés
2. Les arnaques les plus courantes
3. Mails, SMS et messageries piégés
4. Les faux appels et les faux conseillers
5. Mots de passe et double authentification
6. Téléphone, ordinateur et achats en ligne
7. Bénévoles : les données et l'argent du club
8. Réseaux sociaux et vie privée
9. Victime d'une arnaque : que faire ?

Vous n'êtes pas une cible trop petite, au contraire

Votre identité

Votre nom, votre adresse, votre date de naissance ou une copie de votre pièce d'identité permettent d'ouvrir des comptes ou de souscrire des crédits à votre place.

Votre argent

Un virement obtenu sous la pression, un code bancaire communiqué au téléphone ou un faux achat en ligne et l'argent part en quelques minutes.

Vos contacts

Un compte piraté sert ensuite à piéger votre famille, vos amis et les membres de votre club, qui vous font confiance.

La confiance du club

Un faux message au nom du club ou de la Fédération peut toucher des centaines de licenciés d'un seul coup.

Les escrocs ne visent pas les personnes riches ou célèbres, ils visent tout le monde, en espérant tomber sur quelqu'un au mauvais moment.

Les arnaques que l'on rencontre vraiment au quotidien

Le faux message

Un mail, un SMS ou un message WhatsApp qui imite un organisme connu pour vous faire cliquer, payer ou donner vos codes.

Le faux conseiller

Un appel d'un soi-disant conseiller bancaire, d'un service des fraudes ou d'un technicien, très bien informé et très pressant.

Le faux proche

Un enfant, un petit-enfant ou un ami qui aurait changé de numéro et qui a besoin d'argent rapidement.

Le faux site marchand

Une boutique en ligne aux prix imbattables qui encaisse le paiement et n'envoie jamais rien.

Le faux support technique

Un message qui bloque votre écran et vous demande d'appeler un numéro ou d'installer un logiciel pour « réparer ».

L'arnaque aux sentiments

Une relation nouée en ligne, patiemment entretenue, qui finit toujours par une demande d'argent.

D'autres arnaques qui visent directement votre argent

Le faux placement

Un placement présenté comme sûr et très rentable, en crypto-actifs, en or ou en biens divers, proposé par un site ou un démarcheur.

Le bon réflexe

Vérifier l'agrément de l'intermédiaire et les listes noires de l'AMF avant d'investir le moindre euro.

Le faux gain ou le faux héritage

« Vous avez gagné », « vous êtes bénéficiaire d'une succession », avec des frais à régler avant de toucher la somme.

Le bon réflexe

On ne paie jamais pour recevoir un gain ou un héritage.

Le faux service client

Un numéro trouvé sur un moteur de recherche ou un compte sur un réseau social qui se fait passer pour votre banque ou votre fournisseur.

Le bon réflexe

Utiliser seulement les coordonnées de votre contrat, de votre carte bancaire ou de l'application officielle.

Le faux site administratif

Un site qui ressemble à celui de l'administration et facture des frais pour une carte grise, un passeport ou un acte d'état civil.

Le bon réflexe

Passer par le site Service Public pour accéder à la démarche officielle.

Et celles qui visent vos comptes ou qui jouent sur la peur

Le chantage à la webcam

« J'ai piraté votre ordinateur et je vous ai filmé, payez ou j'envoie les images à tous vos contacts. » Le message cite parfois l'un de vos anciens mots de passe.

Le bon réflexe

Ne pas répondre, ne pas payer, changer le mot de passe cité et porter plainte en gardant le message.

Le code envoyé « par erreur »

« Désolé, je t'ai envoyé par erreur mon code de sécurité à 6 chiffres, tu peux me le renvoyer ? » Le message vient souvent d'un contact que vous connaissez.

Le bon réflexe

Ne jamais transmettre ce code, même à un ami et activer la vérification en deux étapes dans WhatsApp.

Le QR code piégé

Un autocollant posé sur un horodateur ou dans un lieu public, ou un QR code reçu par message, qui mène vers un faux site de paiement.

Le bon réflexe

Passer la main sur le QR code pour repérer un autocollant, vérifier l'adresse du site affiché et, au moindre doute, passer par l'application officielle.

Toutes ces arnaques jouent sur les mêmes ressorts

L'urgence

« Avant ce soir », « votre compte va être bloqué » : on vous presse pour que vous n'ayez pas le temps de réfléchir.

L'émotion

La peur, l'inquiétude pour un proche ou la joie d'un gain : une émotion forte fait baisser notre vigilance.

L'autorité

Une banque, la police, la Fédération, un président de club : on obéit plus facilement à ceux qui semblent légitimes.

Le secret

« N'en parlez à personne » : l'escroc cherche à vous isoler de ceux qui pourraient vous mettre en garde.

Dès que vous sentez l'un de ces ressorts dans un message ou un appel, prenez le temps de vous arrêter et d'en parler à quelqu'un.

Les signaux qui doivent vous faire tiquer dans un message

De : Service des licences <licences@renouvellement-bridge.net> 1

Objet : Dernier rappel, votre licence sera suspendue sous 24 h 2

Bonjour,

Nous n'avons pas reçu le règlement de votre licence. Sans paiement de 4,90 € avant demain, votre inscription aux tournois sera suspendue. 3

Merci de régulariser dès maintenant en saisissant votre carte bancaire. 4

Régulariser ma licence 5

1. Une adresse d'expéditeur qui ne correspond pas à l'organisme qui se présente, même si le nom affiché est rassurant.
2. Une menace et un délai très court : suspension, blocage, amende majorée.
3. Un petit montant, qui paraît anodin et que l'on règle sans trop réfléchir.
4. Une demande de coordonnées bancaires ou de codes, directement depuis le message.
5. Un bouton ou un lien dont l'adresse réelle n'apparaît qu'en le survolant, sans cliquer.

SMS et WhatsApp : les scénarios qui reviennent le plus

Le colis en attente

« Votre colis n'a pas pu être livré, des frais de réexpédition sont à régler. »

Le bon réflexe

Ne pas cliquer et suivre ses colis depuis le site du transporteur.

L'amende ou la facture

« Vous avez une amende impayée » ou « votre carte Vitale expire ».

Le bon réflexe

Passer uniquement par le site officiel, que l'on saisit soi-même.

Le proche qui a changé de numéro

« Coucou, c'est moi, j'ai perdu mon téléphone, voici mon nouveau numéro. »

Le bon réflexe

Rappeler la personne sur son numéro habituel avant toute chose.

Un SMS frauduleux ? Transférez-le gratuitement au 33700 pour le signaler, puis supprimez-le.

Au téléphone, l'escroc est souvent poli, rassurant et très bien informé

Le faux conseiller bancaire

Il signale une opération suspecte et vous demande de valider une « annulation » sur votre application, ou de lui donner un code reçu par SMS.

Le faux policier ou le faux service des fraudes

Il vous explique qu'il faut mettre votre argent « à l'abri » sur un autre compte, ou remettre votre carte à un coursier.

La voix imitée

Les outils d'intelligence artificielle permettent aujourd'hui d'imiter la voix d'un proche à partir de quelques secondes d'enregistrement.

Le bon réflexe ne change jamais : vous raccrochez puis vous rappelez vous-même votre banque ou votre proche, sur le numéro que vous connaissez déjà.

Un bon mot de passe n'est pas forcément un mot de passe compliqué

Ce que recommande la CNIL

12 caractères au minimum, en mélangeant majuscules, minuscules, chiffres et caractères spéciaux

ou bien

7 mots au minimum pour une phrase de passe, plus facile à retenir et tout aussi robuste

Pour un mot de passe utilisé seul, sans autre mesure de protection

Ce qui fragilise

Le même mot de passe partout, le prénom d'un petit-enfant suivi d'une date, un carnet posé à côté de l'ordinateur ou un mot de passe confié à quelqu'un.

Ce qui protège

Un mot de passe différent pour chaque compte important, en commençant par la messagerie et la banque et un gestionnaire de mots de passe pour tout retenir.

La double authentification, une deuxième serrure sur vos comptes

Vous saisissez votre mot de passe

C'est la première serrure, celle qu'un escroc peut voler.

Vous confirmez sur votre téléphone

Un code ou une validation dans une application, que vous seul recevez.

Vous accédez à votre compte

Sans votre téléphone, un mot de passe volé ne suffit plus.

Un code ou une demande de validation que vous n'avez pas demandé ?

Ne le transmettez à personne et ne validez rien. Quelqu'un connaît sans doute votre mot de passe : changez-le dès que possible.

Quelques habitudes simples pour vos appareils

Accepter les mises à jour

Elles corrigent des failles déjà connues des escrocs. Les reporter indéfiniment, c'est laisser une fenêtre ouverte.

Verrouiller son téléphone

Un vrai code de verrouillage, pas une date de naissance, protège tout ce que contient votre téléphone en cas de perte ou de vol.

Installer avec prudence

Des applications uniquement depuis les magasins officiels et jamais un logiciel demandé par quelqu'un qui vous appelle.

Se méfier des Wi-Fi publics

Dans un hôtel, une gare ou une salle de tournoi, on évite les opérations bancaires sur un Wi-Fi ouvert.

Si un message bloque votre écran et vous demande d'appeler un numéro, n'appelez pas : fermez le navigateur ou redémarrez l'appareil.

Acheter et payer en ligne sans mauvaise surprise

1



Vérifier la boutique

Une adresse de site qui ressemble à une marque connue, des prix bien trop bas ou aucune mention légale doivent vous faire douter.

2



Payer de façon traçable

La carte bancaire avec validation sur votre application plutôt qu'un virement, des cartes cadeaux ou des coupons demandés par le vendeur.

3



Entre particuliers

Se méfier d'un acheteur qui propose de payer plus que prévu, ou qui vous envoie un lien pour « recevoir » votre argent.

Pour recevoir de l'argent, vous n'avez jamais besoin de saisir votre numéro de carte bancaire ou un code de validation.

Les données des membres sont confiées au club, elles ne lui appartiennent pas



Une donnée personnelle, c'est toute information qui permet d'identifier quelqu'un

Un nom, une adresse mail, un numéro de téléphone ou de licence, mais aussi un classement, un résultat de tournoi ou une photo prise au club.



La copie cachée pour les envois groupés

Mettre les adresses des membres en copie cachée (Cci), pour que chacun ne voie pas celles de tous les autres.



Ne garder que le nécessaire

Une liste à jour, partagée seulement avec ceux qui en ont besoin et supprimée quand elle ne sert plus.



Attention aux supports

Une clé USB, un ordinateur personnel ou un classeur papier qui contient la liste des membres se protège et ne se laisse pas traîner.

Quand on demande au club de payer ou de changer un RIB

Le faux président

Un message du président ou d'un membre du bureau, en déplacement et injoignable, qui demande au trésorier un paiement urgent et discret.

Le bon réflexe

Appeler la personne sur son numéro habituel et respecter les règles de validation du club, même sous pression.

Le faux fournisseur

Un traiteur, une salle ou un fournisseur habituel annonce un changement de coordonnées bancaires, avec un RIB qui semble authentique.

Le bon réflexe

Ne jamais modifier un RIB sur la seule foi d'un mail et le faire confirmer par téléphone auprès d'un contact connu.

Les accès partagés

Les accès au compte bancaire, à la messagerie ou au site du club se transmettent de bénévole en bénévole, parfois depuis des années.

Le bon réflexe

Savoir qui a quels accès, changer les mots de passe quand un bénévole quitte sa fonction et activer la double authentification.

Ce que l'on publie en ligne sert aussi aux escrocs

Votre entourage

Les prénoms de vos enfants et petits-enfants, vos amis, votre club : de quoi rendre un faux message très crédible.

Vos informations personnelles

Une date de naissance, une adresse ou le nom de votre animal servent parfois de réponse aux questions de sécurité.



Ce qu'un escroc peut apprendre en lisant simplement vos publications

Vos absences

Un festival de bridge, des vacances ou un séjour à l'hôpital annoncés en direct indiquent que vous n'êtes pas chez vous.

Vos habitudes

Les lieux que vous fréquentez, vos horaires et vos achats donnent des indices très concrets à qui veut vous piéger.

Les premiers réflexes, sans attendre et sans honte

1	**Prévenir sa banque immédiatement**	Faire opposition sur la carte et signaler les opérations suspectes, même en dehors des heures d'ouverture.
2	**Changer ses mots de passe**	En commençant par la messagerie et le compte concerné, depuis un appareil de confiance.
3	**Prévenir ses contacts**	Si votre messagerie ou votre WhatsApp a été piraté, pour qu'ils ne se fassent pas piéger à leur tour.
4	**Garder les preuves**	Captures d'écran, messages, numéros, références de virement : ne rien supprimer avant d'avoir porté plainte.
5	**Porter plainte**	Auprès de la police ou de la gendarmerie, avec tous les éléments que vous avez gardés.

Vers qui se tourner pour être aidé

17Cyber

Le service public d'assistance en ligne aux victimes de cybermalveillance, ouvert jour et nuit, avec un diagnostic de votre situation et la possibilité d'échanger avec un policier ou un gendarme.

Le premier réflexe en cas de doute ou d'arnaque.

Le 33700

Le numéro gratuit pour signaler un SMS frauduleux en le transférant tel quel, ou un appel douteux en envoyant « spam vocal » suivi du numéro.

Vos signalements aident à faire couper ces numéros.

Vos proches et le club

Pour en parler, vérifier un message douteux avant d'agir ou prévenir les autres membres quand une arnaque circule au nom du club.

Parler d'une tentative, c'est souvent protéger quelqu'un d'autre.

Ce que je vous propose de garder en tête

Prendre le temps quand un message vous presse

Rappeler soi-même sur un numéro que l'on connaît

Ne jamais transmettre un code ou un mot de passe

En parler à un proche ou au club avant d'agir

Merci pour votre attention, place à vos questions