ACADÉMIE
DE BORDEAUX

Liberté
Égalité
Fraternité

Centre Opérationnel de Sécurité des Systèmes d'Information

#1 mars 2022

Le flash
Securité Numérique
prévention des risques cyber dans l'académie de Bordeaux

La cyber-vigilance, c'est l'affaire de tous...

Les cybermenaces sont des **tentatives malveillantes** destinées à perturber les systèmes informatiques jusqu'à les rendre inopérants. Les outils numériques de l'académie de Bordeaux ne sont pas épargnés et il nous appartient à tous conjointement de prendre les mesures tant collectives qu'individuelles pour nous prémunir et garantir la disponibilité continue et le bon fonctionnement de nos outils de travail. **La menace est encore plus forte en ces moments de fortes tensions internationales.**

Les **attaquants** agissent par intrusion (attaque des serveurs), chantage (ransomware), monétisation de données (revente d'informations personnelles) ou vol et usurpation d'identité (phishing). Ils parviennent jusqu'à vous **le plus souvent par la messagerie électronique**.

Prudence !

Dans ce numéro, vous trouverez quelques gestes simples à effectuer couramment dans vos usages professionnels du numérique.

Patrick BENAZET
Responsable de la Sécurité des Systèmes d'Information
de l'académie de Bordeaux

Attaques

130 millions

de tentatives d'**intrusion** dans le système d'information académique répertoriées en **1 an**

Parade

100 %

des tentatives d'**intrusion** sont déjouées par les dispositifs de protection

Piratages

27

C'est le nombre de **comptes** des agents de l'académie **piratés sur un jour** ces dernières semaines

Facteur humain

100 %

Des cas de piratage ont pour origine un **manque de vigilance** dans le traitement d'un courriel reçu sur la messagerie académique

ACADÉMIE
DE BORDEAUX
Liberté
Égalité
Fraternité

Redoublez de vigilance dans le traitement de vos courriels

1

➜ Repérez les indices qui caractérisent un message frauduleux, comme par exemple l'orthographe, l'absence des accents dans le texte, l'adresse de l'expéditeur qui se cache derrière un intitulé en apparence valide, ou encore le nom de la pièce-jointe.
➜ Ne répondez jamais aux demandes de renseignements personnels ou confidentiels, réfléchissez bien avant de saisir votre identifiant ou votre mot de passe.
➜ Signalez systématiquement les messages suspects en les transférant à alerte.messagerie@ac-bordeaux.fr puis supprimez-les.

Un doute ?

alerte.messagerie@ac-bordeaux.fr

Centre Opérationnel de Sécurité des Systèmes d'Information de l'académie de Bordeaux
5, rue Joseph de Carayon-Latour CS 81499
33060 Bordeaux Cedex
Mél : dsi-cos@ac-bordeaux.fr

ACADÉMIE
DE BORDEAUX
Liberté
Égalité
Fraternité

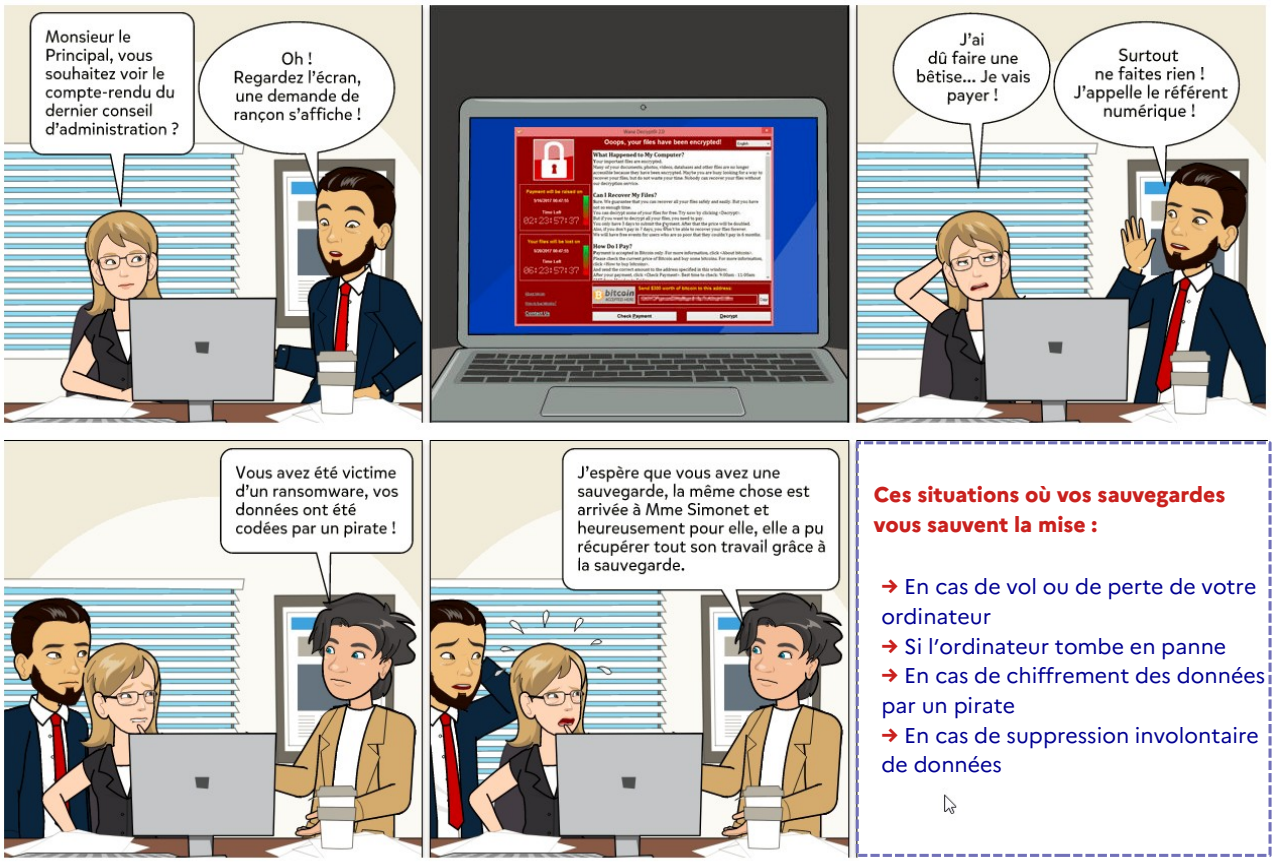
Pensez à faire des copies de sauvegarde de vos documents à fréquence régulière

2

➜ Si vous travaillez au rectorat ou en DSDEN, vos documents sont **automatiquement sauvegardés**. Pour cela il faut **absolument les enregistrer** sur le disque « **X :** » et non pas dans le dossier « Documents ». Cette pratique vaut également en distanciel lorsque vous vous connectez au VPN avec votre OTP.

➜ Si vous ne travaillez pas au rectorat ou en DSDEN, veillez à dupliquer **manuellement** vos documents sur un **support externe** exclusivement dédié : clé USB, disque dur externe, etc.

Dans tous les cas, ne conservez pas vos sauvegardes au même endroit que votre ordinateur !



Ces situations où vos sauvegardes vous sauvent la mise :

➜ En cas de vol ou de perte de votre ordinateur
➜ Si l'ordinateur tombe en panne
➜ En cas de chiffrement des données par un pirate
➜ En cas de suppression involontaire de données

En cas d'incident

Il est possible de restaurer les documents sauvegardés

En faisant un signalement sur la plateforme AMERANA

Centre Opérationnel de Sécurité des Systèmes d'Information de l'académie de Bordeaux
5, rue Joseph de Carayon-Latour CS 81499
33060 Bordeaux Cedex
Mél : dsi-cos@ac-bordeaux.fr

ACADÉMIE
DE BORDEAUX
Liberté
Égalité
Fraternité

Comment les pirates opèrent-ils pour altérer vos données et vos outils numériques ?

3

Voici **4 exemples** qui font appel à des techniques désormais régulièrement relevées qui ont pour objectif de **récupérer vos données de connexion** en vue d'une intrusion ultérieure dans le système d'information par **usurpation d'identité** ou bien de tenter de **vous extorquer des fonds** par chantage et menace.

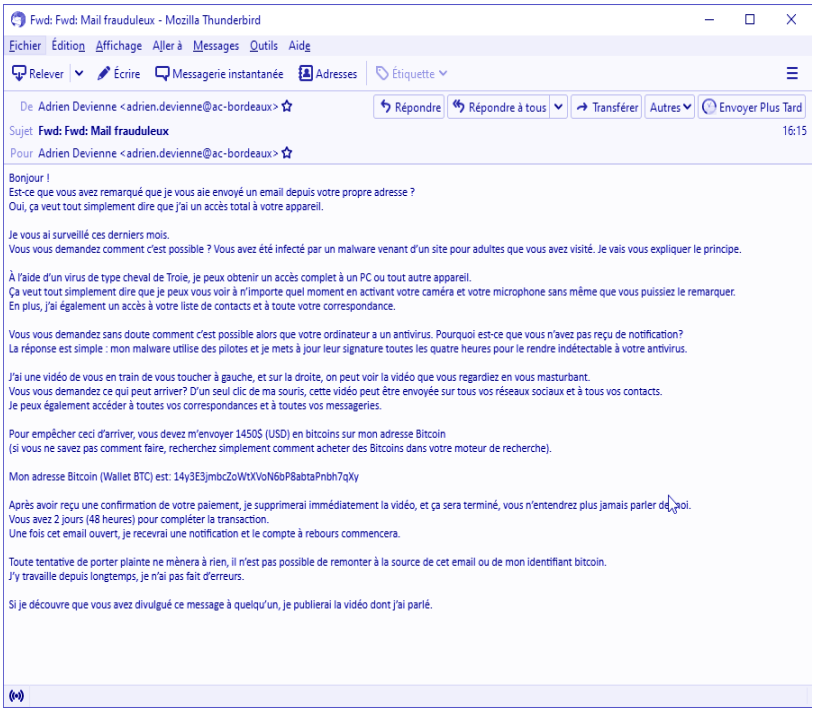
Dans cet exemple, le cybercriminel essaie de faire peur en usurpant l'identité d'une instance judiciaire dans l'intention de soutirer des informations personnelles au destinataire du message.

Transférez ce type de message à alerte.messagerie@ac-bordeaux.fr
puis mettez-le à la corbeille

Ici, le pirate demande au destinataire du message de cliquer sur un lien qu'il fait passer pour l'application I-Prof dans le but de lui dérober son identifiant et son mot de passe pour ensuite usurper son identité.

Ne cliquez surtout pas sur ce genre de lien, transférez ce type de message à alerte.messagerie@ac-bordeaux.fr puis mettez-le à la corbeille

Centre Opérationnel de Sécurité des Systèmes d'Information de l'académie de Bordeaux
5, rue Joseph de Carayon-Latour CS 81499
33060 Bordeaux Cedex
Mél : dsi-cos@ac-bordeaux.fr



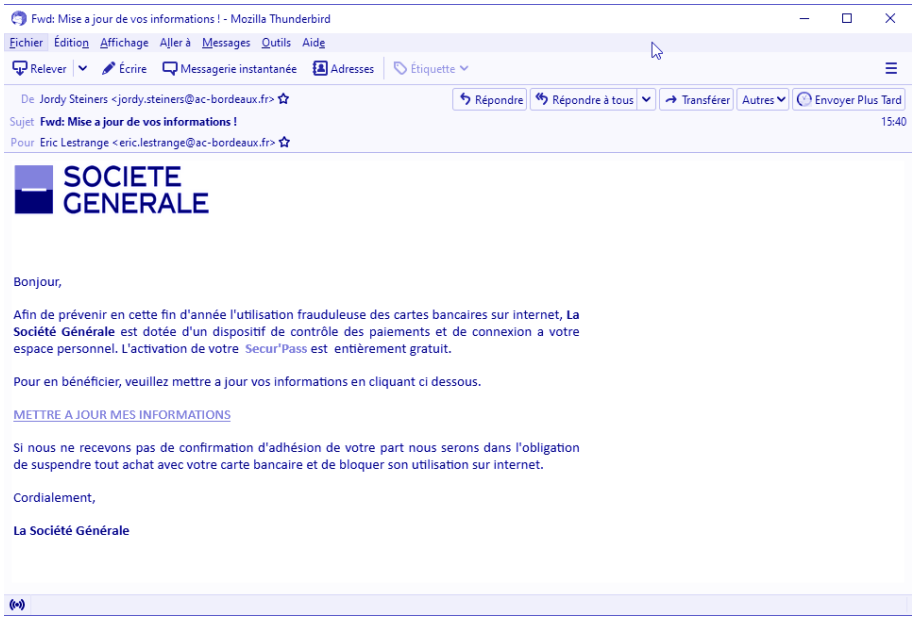
Dans ce cas, l'intimidation est utilisée par le cybercriminel au travers d'arguments en apparence techniques qui tendent à faire croire que ses allégations sont fondées.
Il exige une rançon en échange du silence du destinataire du message au regard de ses prétendus agissements qui sont naturellement totalement inventés.
Un forte pression est mise sur le destinataire du message par l'annonce d'un délai de mise à exécution très court.

Ne prenez jamais ce genre de message au sérieux, transférez-le à alerte.messagerie@ac-bordeaux.fr et mettez-le à la corbeille.

De manière générale, ne payez jamais de rançon.

A travers cet exemple, on voit comment un pirate se fait passer pour un organisme bancaire en falsifiant un message graphiquement structuré comme un original par lequel il invite à se connecter sous prétexte d'une nécessaire sécurisation de l'accès au compte bancaire.
Le seul objectif est de récupérer l'identifiant et le mot de passe de la victime en vue d'usurper ensuite son identité.

Signalez ce message en le transférant à alerte.messagerie@ac-bordeaux.fr puis mettez-le à la corbeille.



Centre Opérationnel de Sécurité des Systèmes d'Information
de l'académie de Bordeaux
5, rue Joseph de Carayon-Latour CS 81499
33060 Bordeaux Cedex
Mél : dsi-cos@ac-bordeaux.fr

ACADÉMIE
DE BORDEAUX
Liberté
Égalité
Fraternité

Votre mot de passe est un secret, il vous protège mais protège autant les autres

4

Voici **5 principes** à respecter

robustesse

Votre mot de passe est l'unique clé d'accès à toutes vos applications académiques. S'il n'est pas assez complexe, il peut être découvert par des pirates. Il faut donc veiller à ce qu'il comporte au moins 12 caractères, qu'il ne contienne pas de mot du dictionnaire et qu'il soit constitué de lettres majuscules et minuscules, de chiffres et de caractères spéciaux. Idéalement, il ne doit ressembler à rien de particulier, vous êtes libre de choisir la méthode qui vous convient pour le créer.

Le renouvellement régulier de votre mot de passe rend les attaques des cybercriminels plus difficiles. La fréquence préconisée par l'ANSSI est de 3 mois, mais un renouvellement annuel est un bon compromis.

renouvellement

secret

Un mot de passe ne doit jamais être communiqué. En cas d'oubli, il est toujours possible à un administrateur de la DSI de le réinitialiser. Interdisez-vous le post-it collé sous le clavier ou pire sur l'écran. Vous pouvez le noter mais il doit être conservé dans un lieu sûr connu seulement de vous.

Il peut être tentant d'utiliser le même mot de passe pour plusieurs sites. Cette pratique est à proscrire car un cybercriminel qui s'en emparerait pourrait accéder à tous les sites en question.

autant de mots de passe que de sites

verrouillage

Ne laissez jamais votre ordinateur ou votre smartphone sans surveillance avec une session ouverte. Pensez à paramétrer votre écran de verrouillage ce qui empêchera une autre personne d'utiliser votre session, voire de changer votre mot de passe à votre insu.

Centre Opérationnel de Sécurité des Systèmes d'Information
de l'académie de Bordeaux
5, rue Joseph de Carayon-Latour CS 81499
33060 Bordeaux Cedex
Mél : dsi-cos@ac-bordeaux.fr