ALERTE AUX VIRUS !

Une cyberattaque fait l'actualité des systèmes d'information par la propagation massive d'un virus informatique. Ce virus peut passer outre les dispositifs de sécurité en place et provoquer des pertes de données irréversibles. La solution pour limiter voire, empêcher ces dommages passe par la sensibilisation de tous les usagers, notamment dans l'utilisation du courrier électronique.

L'académie n'est pas à l'abri

➤ *Le phénomène et sa manifestation*

Ce virus appartient à la famille des crypto-virus qui en cas d'attaque verrouillent tous les fichiers de votre ordinateur avec une clé de chiffrement tenue secrète, en échange d'une rançon, d'où leur nom de *« rançongiciels »* ou *« ransomware »*. Le virus est véhiculé par mail, dans une pièce jointe, généralement au format .Zip, **si la pièce jointe est ouverte.**

Ce crypto-virus opère en renommant les fichiers présents sur le disque dur de votre ordinateur. Leur nouveau nom est une chaine aléatoire de caractères.
Exemple : FA3D5195-3FE9-1DBC-E35E-89380D21F515. **(crypto-virus)**

Tous les fichiers renommés auront été chiffrés par le virus
et ne seront **plus récupérables si vous ne disposez pas d'une sauvegarde**.

Les services académiques assurent la protection de vos postes de travail ou vous indiquent des recommandations à respecter. En EPLE, assurez-vous auprès de votre administrateur local que votre système d'exploitation Windows et votre navigateur sont mis à jour.

➤ *Que faire si mon pc est victime d'une attaque des crypto-virus*

S'il est connecté à un réseau informatique, débrancher immédiatement le câble réseau ; débrancher tous les périphériques de stockage connectés au pc. Cette action évitera le chiffrage des fichiers présents dans les dossiers partagés sur le réseau et sur les périphériques et limitera **ainsi** la propagation du virus.

N'utilisez plus le poste contaminé et prévenez rapidement vos collègues et votre hiérarchie afin qu'un signalement soit fait auprès des services d'assistance : **cecoia.ac-creteil.fr** ou **cariina 08 20 26 26 26.**

Si un message vous propose la récupération de vos données en échange d'un paiement (rançon), **n'acceptez surtout pas !** N'espérez pas obtenir des pirates les outils nécessaires au déchiffrage de vos fichiers, ils sont trop occupés à élaborer de nouveaux virus.

Aucune solution ne pourra nous protéger face aux actions de l'utilisateur, commises par méconnaissance ou par inadvertance. Il convient donc d'être vigilant face aux mails !

ALERTE AUX VIRUS !

Une cyberattaque fait l'actualité des systèmes d'information par la propagation massive d'un virus informatique. Ce virus peut passer outre les dispositifs de sécurité en place et provoquer des pertes de données irréversibles. La solution pour limiter voire, empêcher ces dommages passe par la sensibilisation de tous les usagers, notamment dans l'utilisation du courrier électronique.

L'académie n'est pas à l'abri

➤ Le phénomène et sa manifestation

Ce virus appartient à la famille des crypto-virus qui en cas d'attaque verrouillent tous les fichiers de votre ordinateur avec une clé de chiffrement tenue secrète, en échange d'une rançon, d'où leur nom de « rançongiciels » ou « ransomware ». Le virus est véhiculé par mail, dans une pièce jointe, généralement au format .Zip, si la pièce jointe est ouverte.

Ce crypto-virus opère en renommant les fichiers présents sur le disque dur de votre ordinateur. Leur nouveau nom est une chaine aléatoire de caractères.
Exemple : FA3D5195-3FE9-1DBC-E35E-89380D21F515. (crypto-virus)

Tous les fichiers renommés auront été chiffrés par le virus
et ne seront plus récupérables si vous ne disposez pas d'une sauvegarde.

Les services académiques assurent la protection de vos postes de travail ou vous indiquent des recommandations à respecter. En EPLE, assurez-vous auprès de votre administrateur local que votre système d'exploitation Windows et votre navigateur sont mis à jour.

➤ Que faire si mon pc est victime d'une attaque des crypto-virus

S'il est connecté à un réseau informatique, débrancher immédiatement le câble réseau ; débrancher tous les périphériques de stockage connectés au pc. Cette action évitera le chiffrage des fichiers présents dans les dossiers partagés sur le réseau et sur les périphériques et limitera ainsi la propagation du virus.

N'utilisez plus le poste contaminé et prévenez rapidement vos collègues et votre hiérarchie afin qu'un signalement soit fait auprès des services d'assistance : cecoia.ac-creteil.fr ou cariina 08 20 26 26 26.

Si un message vous propose la récupération de vos données en échange d'un paiement (rançon), n'acceptez surtout pas ! N'espérez pas obtenir des pirates les outils nécessaires au déchiffrage de vos fichiers, ils sont trop occupés à élaborer de nouveaux virus.

Aucune solution ne pourra nous protéger face aux actions de l'utilisateur, commises par méconnaissance ou par inadvertance. Il convient donc d'être vigilant face aux mails !

Les réflexes à avoir lors de la réception du courrier

➤ ***N'ayez pas une confiance aveugle dans le nom de l'expéditeur***
L'identité d'un expéditeur n'est en rien garantie. N'importe qui peut vous envoyer un courriel en se faisant passer pour un autre. Cela est aussi simple que d'inscrire un faux nom d'expéditeur au dos d'une enveloppe postale.

➤ ***Méfiez-vous des pièces jointes***
N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts.

➤ ***Ne répondez jamais à une demande d'informations confidentielles***
Les demandes d'informations confidentielles, lorsqu'elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, etc.).

➤ ***Si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer***
En passant la souris au-dessus du lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncée dans le message. Si l'adresse est différente, évitez de cliquer sur le lien.

➤ ***Désactivez l'ouverture automatique des documents téléchargés***
Mettez à jour vos logiciels et paramétrez votre logiciel de messagerie pour désactiver la prévisualisation automatique des pièces jointes.

➤ ***N'ouvrez pas et ne relayez pas de messages impersonnels***
Les chaînes de lettre, les appels à la solidarité ou les alertes virales sont souvent porteurs de virus.

➤ ***Soyez vigilant***
Lisez tous les messages au format texte brut avant de cliquer.

Quelques ressources pour faire face

➤ Les EPLE sont systématiquement dotés d'un Antivirus Trend. En revanche, tous les agents de l'EN peuvent bénéficier **gratuitement** du même antivirus à titre personnel, en le téléchargeant : http://eduscol.education.fr/cid92380/renouvellement-du-marche-national-antivirusantispam.htm

➤ Le site de l'ANSSI : http://www.ssi.gouv.fr/entreprise/principales-menaces

➤ Des mesures de prévention et un guide de paramétrage des logiciels de messagerie sont disponibles sur le site du CERT-FR

Les réflexes à avoir lors de la réception du courrier

➤ ***N'ayez pas une confiance aveugle dans le nom de l'expéditeur***
L'identité d'un expéditeur n'est en rien garantie. N'importe qui peut vous envoyer un courriel en se faisant passer pour un autre. Cela est aussi simple que d'inscrire un faux nom d'expéditeur au dos d'une enveloppe postale.

➤ ***Méfiez-vous des pièces jointes***
N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts.

➤ ***Ne répondez jamais à une demande d'informations confidentielles***
Les demandes d'informations confidentielles, lorsqu'elles sont légitimes, ne sont jamais faites par courriel (mots de passe, code PIN, coordonnées bancaires, etc.).

➤ ***Si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer***
En passant la souris au-dessus du lien proposé, vous pouvez repérer s'il pointe bien vers l'adresse du site annoncée dans le message. Si l'adresse est différente, évitez de cliquer sur le lien.

➤ ***Désactivez l'ouverture automatique des documents téléchargés***
Mettez à jour vos logiciels et paramétrez votre logiciel de messagerie pour désactiver la prévisualisation automatique des pièces jointes.

➤ ***N'ouvrez pas et ne relayez pas de messages impersonnels***
Les chaînes de lettre, les appels à la solidarité ou les alertes virales sont souvent porteurs de virus.

➤ ***Soyez vigilant***
Lisez tous les messages au format texte brut avant de cliquer.

Quelques ressources pour faire face

➤ Les EPLE sont systématiquement dotés d'un Antivirus Trend. En revanche, tous les agents de l'EN peuvent bénéficier **gratuitement** du même antivirus à titre personnel, en le téléchargeant : http://eduscol.education.fr/cid92380/renouvellement-du-marche-national-antivirusantispam.htm

➤ Le site de l'ANSSI : http://www.ssi.gouv.fr/entreprise/principales-menaces

➤ Des mesures de prévention et un guide de paramétrage des logiciels de messagerie sont disponibles sur le site du CERT-FR