CSIRT – Hauts-de-France

Centre de réponse aux incidents informatiques

Créé sous l'égide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le CSIRT, fait partie d'un réseau interrégional appelé à développer une culture de cybersécurité de proximité.

Monsieur
Valentin Gruson
Analyste

Pour une sensibilisation aux bonnes pratiques en cybersécurité, présentation des principales menaces actuelles et des moyens de s'en prémunir

13/06/2025

Pourquoi les pirates s'intéressent à VOUS ?

Vol de données personnelles

Nom, adresse, carte bancaire, documents …

Fraude bancaire & usurpation d'identité

Accès à vos comptes, crédits ouverts à votre nom, achats frauduleux…

Pourquoi les pirates s'intéressent à VOUS ?

Accès à vos contacts

Les pirates se font passer pour vous !

Extorsion ou chantage

Photos privées, messages sensibles, documents volés…

Utilisés pour vous faire chanter ou vous intimider.

CSIRT HAUTS-DE-FRANCE

Pourquoi les pirates s'intéressent à VOUS ?

#3/3

Profilage et revente de données

Vos habitudes en ligne tracent un portrait précis de vous…

Parfait pour des arnaques personnalisées et encore plus efficaces.

Comment les pirates s'y prennent ?

Cybermenaces les plus courantes

#1/5

Phishing (hameçonnage)

Faux emails, SMS ou messages vous incitant à cliquer sur un lien piégé ou à donner vos infos personnelles.

“ Votre colis est en attente de paiement ”

Comment les pirates s'y prennent ?

Cybermenaces les plus courantes

🔐 Fuite de mot de passe

Vos mots de passe trop simples ou réutilisés peuvent être récupérés après une fuite de données !

Un seul mot de passe volé = plusieurs comptes compromis !

Comment les pirates s'y prennent ?

Cybermenaces les plus courantes

Applications malveillantes

*Des apps trompeuses installées sur votre téléphone ou ordinateur pour **espionner**, **voler** ou **piéger**.*

Wi-Fi public non sécurisé

Cafés, gares, hôtels… Ces réseaux ouverts sont parfaits pour les pirates.

Comment les pirates s'y prennent ?

Cybermenaces les plus courantes

🎁 Arnaques par colis, fausses factures ou support technique

" Bonjour, c'est Microsoft©*, on a détecté un problème sur votre ordinateur… " Ces techniques jouent sur* ***l'urgence, la peur ou la confiance****. Ne tombez pas dans le piège !*

Comment les pirates s’y prennent ?

Cybermenaces les plus courantes

🛠 Mises à jour oubliées

Un logiciel ou système pas à jour = faille de sécurité ouverte !

Quelles méthodes pour me pirater ?

#1/6

- *L'ingénierie sociale, c'est **l'art de manipuler les gens** au lieu de pirater des machines.*
- *Objectif : vous amener à **révéler des infos sensibles** ou à **faire une action risquée**, sans vous en rendre compte.*

Quelles méthodes pour me pirater ?

Techniques préférées

📨 Phishing

Des emails ou SMS piégés qui vous poussent à cliquer sur un lien ou à entrer un mot de passe ❌🔐.

📞 Vishing (Voice + Phishing)

Un faux conseiller (banque, sécurité informatique…) vous appelle pour “ résoudre un problème urgent ”🎧💬.

Quelles méthodes pour me pirater ?

Techniques préférées

Smishing (SMS + Phishing)

Des messages alarmants :

- *“ Colis bloqué ”,*
- *“ Compte suspendu ”,*
- *“ Amende à payer ”... → pour vous faire cliquer dans la panique.*

Quelles méthodes pour me pirater ?

Techniques préférées

🛠 Faux support technique

Une fenêtre surgit sur votre écran :

“ Votre PC est infecté ! ” 😱

On vous demande d’installer un logiciel ou de payer un dépannage imaginaire.

Quelles méthodes pour me pirater ?

Techniques préférées

#5/6

Usurpation d'identité / Faux profils

Quelqu'un se fait passer pour ***un collègue****,* ***un proche ou un prestataire*** *pour* ***gagner votre confiance*** *… et vous piéger.*

Quelles méthodes pour me pirater ?

Techniques préférées

Fichiers piégés

Une pièce jointe ou un lien dans un email… vous cliquez et sans le savoir, vous installez un logiciel malveillant .

Qui peut me pirater ?

#1/5

💰 Cybercriminels “ classiques ”

Leur but ? L’argent, toujours l’argent !

Ils volent vos données bancaires, identifiants ou vous rançonnent via des ransomwares.

Qui peut me pirater ?

Arnaqueurs opportunistes

Ce sont les petits escrocs du net.

Ils envoient du phishing, des fausses factures ou des SMS trompeurs à la chaîne, en espérant que quelqu'un morde à l'hameçon.

Qui peut me pirater ?

🎭 Hacktivistes

Motivés par des causes sociales ou politiques, ils attaquent des entreprises ou institutions symboliques.

Moins intéressés par l'argent, plus par le message.

Qui peut me pirater ?

Cyberespions & États-nations

Utilisent des outils très avancés pour surveiller ou voler des infos stratégiques.

Peu probable en tant que particulier… sauf si votre entourage ou métier est sensible.

Qui peut me pirater ?

Script kiddies (pirates débutants)

Jeunes curieux ou amateurs qui testent des outils de piratage qu'ils n'ont pas créés.

Leurs motivations ? Apprendre, s'amuser ou parfois ***faire des dégâts involontaires****.*

Darknet, mes données volées : que deviennent-elles ?

#1/7

- *Ce n'est pas qu'un mythe de films : le **Darknet** est une partie cachée d'Internet, inaccessible par les moteurs de recherche classiques, souvent utilisée pour des activités illégales… mais pas uniquement.*

Darknet : quelles données y retrouve-t-on ?

Identifiants et mots de passe

emails, réseaux sociaux, comptes bancaires…

Données personnelles

nom, adresse, numéro de téléphone, carte d'identité, etc.

Darknet : quelles données y retrouve-t-on ?

Informations bancaires

numéros de carte, RIB, identifiants de paiement

Dossiers médicaux

ou documents administratifs

Darknet : quelles données y retrouve-t-on ?

Photos, vidéos, données intimes

utilisées pour du chantage (sextorsion)

Darknet : Comment sont-elles vendues ?

🖷 Packs de données vendus par lot

“ 10 000 comptes Gmail pour 30 € ”

📈 Prix variables

selon la fraîcheur, la rareté, ou l’accès potentiel offert

Darknet : Comment sont-elles vendues ?

- **Utilisées dans des campagnes automatisées**

  phishing, arnaques, fraudes

Darknet : mythe ou réalité ?

✓ **Réalité**

oui, des données fuitées ou volées s'y retrouvent

✗ **Mais tout n'est pas " hacker hollywoodien "**

souvent le résultat d'un manque de vigilance (mots de passe faibles, clics sur de faux liens, etc.)

Comment me protéger des pirates ?

#1/10

❶ Utilisez des mots de passe solides et uniques

➡ *Longs, complexes, et différents pour chaque compte / Activez la double authentification (2FA) / Utilisez un gestionnaire de mots de passe*

Comment me protéger des pirates ?

❷ Sauvegardez vos données régulièrement 💾

➡ *Clé USB, disque dur externe ou cloud sécurisé*

Comment me protéger des pirates ?

❸ Méfiez-vous des messages suspects

➡ *Ne cliquez pas trop vite sur un lien ou une pièce jointe douteuse / Vérifiez toujours l'expéditeur*

Comment me protéger des pirates ?

❹ Méfiez-vous des messages suspects 💻⚙🔄

➡ *Les mises à jour corrigent les failles de sécurité /*

Installez un antivirus fiable

Comment me protéger des pirates ?

❺ Évitez les réseaux Wi-Fi publics non sécurisés

➡ *Ces réseaux ouverts sont des terrains de chasse pour les cybercriminels.*

Connexion facile, intrusion tout aussi simple.

Comment me protéger des pirates ?

❻ Séparez les usages (pro et perso) 💼

➡ *Un appareil pour chaque usage = moins de risques.*

Comment me protéger des pirates ?

❼ Restez loin des sites douteux ou illégaux ⊘

➡ *Cliquez malin, évitez ces sites*

Ils peuvent compromettre votre sécurité et votre vie privée.

Comment me protéger des pirates ?

#8/10

❽ Restez loin des sites douteux ou illégaux 📥

➡ *Téléchargez uniquement depuis des sources officielles.*

Comment me protéger des pirates ?

#9/10

❾ Réfléchissez avant de publier des infos perso 🙊

➡ *Nom, adresse, job, photo… ces données intéressent les pirates !*

Comment me protéger des pirates ?

#10/10

⑩ Formez-vous et sensibilisez vos proches 🎓

➡ *Plus vous êtes informé, mieux vous êtes protégé…*

et vous protégez les autres ! 👬

Services étatiques pour m'aider

#1/3

- **Forces de l'ordre spécialisées**

  ➡ *Centre de lutte contre les criminalités numériques C3N (Gendarmerie)*

  ➡ *Office anti-cybercriminalité OFAC (Police nationale)*

Services étatiques pour m'aider

- **CSIRT Hauts-de-France**

  ➡ *Équipe régionale de réponse aux incidents cyber*

  ➡ *Gratuit & local : pour associations, PME, collectivités, établissements publics*

  ➡ *Aide à gérer un incident (analyse, urgence, conseils)*

  ➡ *Aide à se renforcer face aux menaces numériques*

Services étatiques pour m'aider

- **Cybermalveillance.gouv.fr**

  ➡ *Le portail national pour les victimes de cybermalveillance*

  ➡ *Conseils, prévention, signalements et ressources utiles*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

CSIRT
HAUTS-DE-FRANCE

EN CAS DE CYBERATTAQUE APPELEZ LE :

0806 700 111

CSIRT HAUTS-DE-FRANCE — Soutenu par — RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité — Région Hauts-de-France — CITC DIGITAL INNOVATION HUB HAUTS-DE-FRANCE — EDIH GREEN POWER IT EUROPEAN DIGITAL INNOVATION HUB HAUTS-DE-FRANCE — Cofinancé par l'Union européenne

La Région Hauts-de-France s'engage en faveur de la Cybersécurité