CENTRE DE RESSOURCES CYBERSÉCURITÉ

L'HAMEÇONNAGE

Dordogne PÉRIGORD LE DÉPARTEMENT dordogne.fr

atd 24 AGENCE TECHNIQUE DÉPARTEMENTALE

CCI DORDOGNE

SOMMAIRE

CRC 24
CENTRE DE RESSOURCES CYBERSÉCURITÉ

LE CENTRE DE RESSOURCES EN CYBERSECURITE

OBJECTIFS DU CRC24

- assurer une **résilience territoriale**
- renforcer la **confiance numérique**

4 AXES D'INTERVENTION POUR LE CRC24

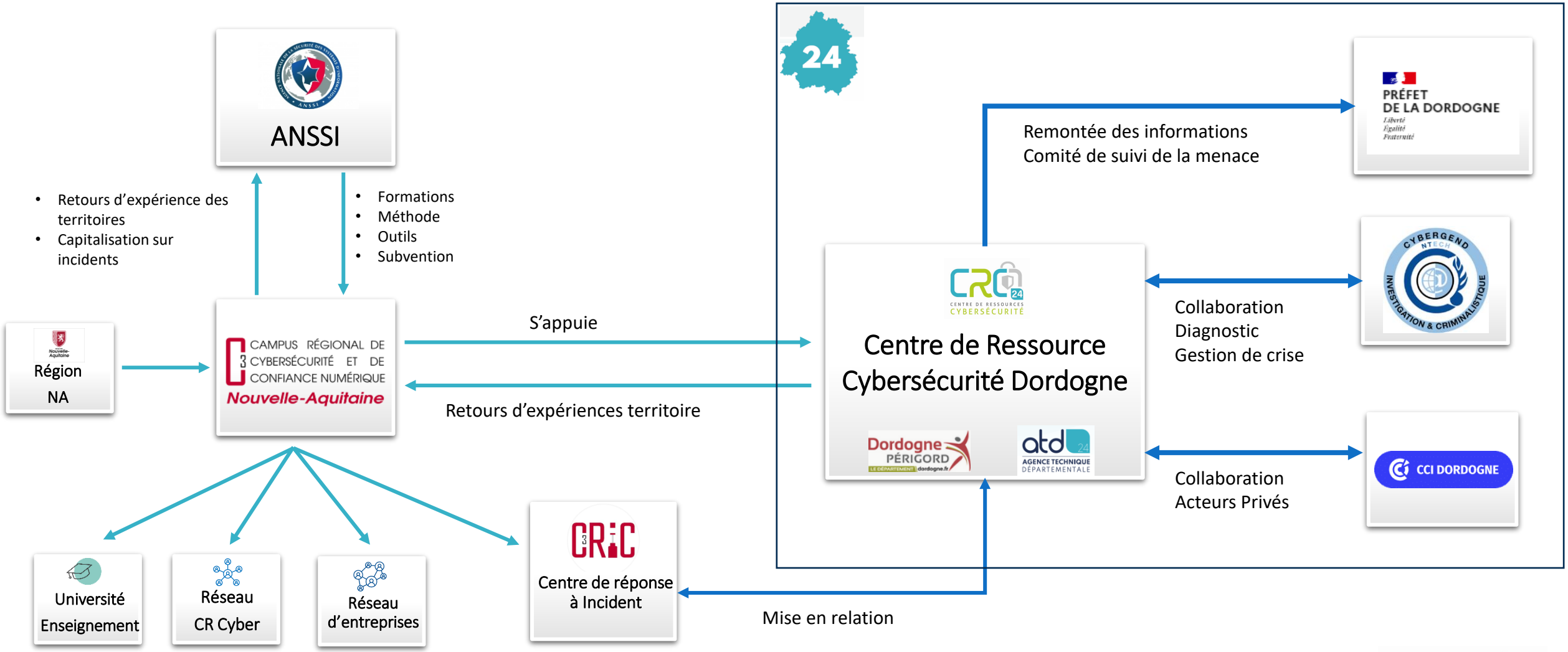
- Les **opérations**
- La **sensibilisation**
- La **formation**
- **L'accompagnement en cas de crise**

UN ACCOMPAGNEMENT COMPLET

- **Se protéger/Prévenir**
- **Gérer un incident**
- **Revenir à la normale**

CRC 24
CENTRE DE RESSOURCES CYBERSÉCURITÉ

LE CENTRE DE RESSOURCES EN CYBERSECURITE

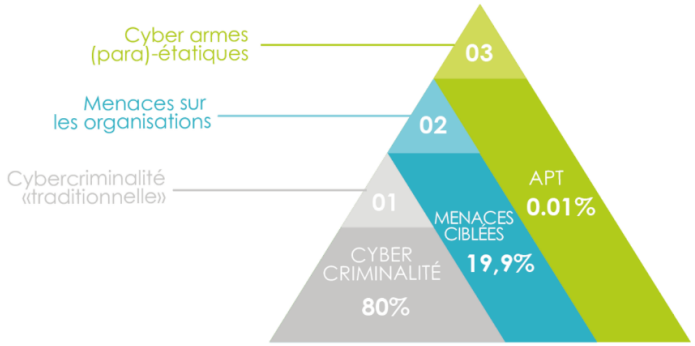


01 | LE CONTEXTE CYBERSECURITE ACTUEL

TOP 10 des principaux risques en France

Rank		Percent	2023 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	44%	*1 (40%)*	→
2	Business interruption *(incl. supply chain disruption)*	40%	*2 (32%)*	→
3	Fire, explosion	25%	*7 (20%)*	↑
4	Climate change *(e.g., physical, operational, and financial risks as a result of global warming)*	23%	*6 (22%)*	↑
5	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	22%	*5 (23%)*	→
6	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil commotion, strikes, riots, looting)*	21%	NEW	↑
7	Changes in legislation and regulation *(e.g., tariffs, economic sanctions, protectionism, Euro-zone disintegration)*	16%	*8 (15%)*	↑
8	Energy crisis *(e.g., supply shortage / outage, price fluctuations)*	15%	*3 (28%)*	↓
9	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	14%	*4 (24%)*	↓
10	Critical infrastructure blackouts *(e.g., power disruption)* or failures *(e.g., aging dams, bridges, rail tracks)*	13%	NEW	↑

UNE MENACE PROTÉIFORME



QUELQUES CHIFFRES

- 450 millions d'attaques pour les JO de Tokyo, on s'attend à 8 à 10 fois plus pour les JO de PARIS ;
- **Panorama de la menace 2023 – ANSSI** :
  Top 5 des victimes par rançongiciel (pris en otage du système contre une rançon) :
  1 : TPE/PME/ETI : 34% ↓
  2 : Collectivités territoriales : 24% ↑
  3 – 4 : Entreprises Stratégiques – Etablissement de Santé : 10% ↑
  5 : Association : 9% ↑

CRC 24 CENTRE DE RESSOURCES CYBERSÉCURITÉ

02 | LES MOTIVATIONS DES PIRATES

ATTAQUE A BUT LUCRATIF

Principales menaces, elles prennent diverses formes : attaques par rançongiciels, attaque point d'eau, compromission de messageries professionnelles…

ATTAQUE A BUT DE DESTABILISATION

Elles consistent en une défiguration des sites internet à des fins politiques ou idéologique ("hacktivisme") et par des attaques à but de sabotage.

ATTAQUE A BUT D'ESPIONNAGE

Visant à compromettre les équipements informatiques afin d'espionner les cibles visées. Ces attaques sont réalisées majoritairement par des groupes opérant pour le compte d'États.

CRC 24
CENTRE DE RESSOURCES CYBERSÉCURITÉ

03 | LES TECHNIQUES DE PHISHING

LES EMAILS DE PHISHING

Les attaquants se font passer pour des entités de confiance et créent des courriels convaincants qui semblent souvent urgents ou importants

BUT

Obtenir un accès non autorisé à des données sensibles

Commettre une usurpation d'identité

Mener d'autres activités malveillantes

LE SPEAR PHISHING

Les attaquants personnalisent leurs techniques d'attaque pour faire passer les courriels ou les messages frauduleux pour des messages légitimes et dignes de confiance

BUT

Recueillir des informations sur les cibles afin d'élaborer des courriels personnalisés

Voler des identifiants de connexion

LE PHISHING PAR QR CODE

Les attaquants génèrent un QR code renvoyant vers un site frauduleux ou un logiciel malveillant. Le QR code est placé dans un lieu public ou envoyé par mail

BUT

Recueillir des informations sur les cibles

Récupérer des données personnelles ou financières

Infecter les appareils ayant scanner le QR Code

LE SMS PHISHING

Les attaquants se font passer pour des entités connues, de confiance et créent des SMS convaincants

BUT

Recueillir des informations sur les cibles

Récupérer des données personnelles, des identifiants de connexion ou des données financières

Infecter les téléphones

04 | COMMENT SE PROTEGER ?

Ne jamais communiquer d'informations sensibles par mail, téléphone ou sur Internet. Aucune structure « de confiance » ne doit demander de telles informations à distance.

Pour vérifier le lien contenu dans le message, on passe la souris dessus **SANS CLIQUER**, l'adresse du lien s'affichera et permettre de contrôler sa fiabilité.

En cas de doute sur le lien, copier le lien pour le coller dans la barre d'adresse du navigateur ce qui permettra de vérifier le site.

Utiliser des **mots de passe différents** sur les sites et/ou application.

Activer, dès que possible et si le site le permet, **la double authentification**.

05 | QUE FAIRE EN CAS DE PHISHING AVERE

Au moindre doute, contactez l'administration ou l'entreprise qui est censée avoir adressé le mail ou SMS pour confirmer le message reçu. Vous trouverez ses coordonnées sur son site Internet officiel

En cas de diffusion de mots de passe et/ou d'informations sensibles (compte bancaire par exemple) **: changer les mots de passe rapidement, alerter votre banque, faite opposition : il faut réagir rapidement.**

Si vous avez cliqué sur un lien qui a pu installer **une application malveillante et/ou si vous constatez des comportements anormaux sur vos appareils** : évitez de réaliser des opérations sensibles, déconnectez internet, supprimez les applications installées, restaurez ou réinstallez le système de l'appareil en dernier recours.

Déposer plainte en apportant les preuves en votre possession : mail, date/heure et numéro de l'appel…

Signaler sur des plateformes dédiées et identifiées :
Pour les faux mails : https://phishing-initiative.fr/contrib/
Ou alerter votre service informatique si c'est dans votre environnement professionnel

06 | COMMENT RECONNAIRE UNE TENTATIVE DE PHISHING ?

Les messages phishing sont quasi-identiques aux messages provenant de l'identité usurpé, il peut y avoir des signaux à repérer :

- **Notifications** de votre système de messagerie ou des systèmes de sécurité (antivirus, antispam…). Il est important de prendre en considération les éventuelles alertes.
- Un email provenant d'un **expéditeur inconnu :** les pirates procèdent généralement au hasard en mode pêche au chalut, au cas où une personne se ferait avoir.
- **Une correspondance nom & adresse mail fantaisiste** : certains mails de phishing ont un nom d'expéditeur plutôt fiable mais une adresse mail totalement fantaisistes.
- **Un objet alarmiste ou trop alléchant : «** remboursement » ou « alerte de sécurité » provoquant un sentiment d'urgence.
- **Des demandes inhabituelles**
- **Des demandes d'informations confidentielles**
- **Une incitation à cliquer sur un lien ou un pièce-jointe**

06 | COMMENT RECONNAIRE UNE TENTATIVE DE PHISHING ?

impots.gouv.fr
un site de la Direction générale des Finances publiques

Cher (e) Client (e)

Apres les derniers calculs annuels de l'exercice de votre activité,
nous vous déterminons que vous admissible a recevoir un remboursement de 120.80 Euro

Veuillez nous soumettre s'il vous plait la demande de remboursement d'impôt

pour nous permettre de la traiter dans un plus bref délai
(le délai du traitement est de 10 jours ouvert).

>> Pour acceder au formulaire pour votre remboursement d'impôt , cliquez ici .

Un remboursement peut être retarde pour diverses raison . Par exemple

la soumission du dossier non valides ou inscriptions après une certaine limite

Le Conciliateur fiscal adjoint
Philippe BERGER

Vous étés tenu de fournir un numéro de téléphone ou notre conseil pourra vous joindre .

Nous vous prions d'accepter nos excuses .

Crédit Agricole <hotlinesbo@resepku.online>
Information : Nous venons de désactiver votre carte de crédit.
À

BANQUE ET ASSURANCES

Bonjour .

Nous venons de désactiver votre carte de crédit.

Nous avons détecté plusieurs IP connectons à votre compte Banque Crédit Agricole et des multiples erreurs de mot passe avant l'ouverture de session.
Pour le réactiver, vous devez vous connecter sur le site de La Banque Crédit Agricole et accéder à votre espace sécurisé de Banque en ligne via le lien ci-dessous

La procédure est très simple :

1. Cliquez sur le lien ci-dessous pour ouvrir une fenêtre de navigateur sécurisée.
2. Confirmez que vous êtes bien le titulaire du compte et suivez les instructions.

Accéder à votre compte

Ce message est généré automatiquement ne répond pas à l'expéditeur.
Si vous n'êtes pas destinataire(s) de ce message merci de le détruire.

Compte Ameli : nous avons déterminé que vous recevrez un remboursement de 850,99 €. Veuillez remplir votre formulaire de remboursement et confirmez-le via le lien ci-dessous : https://bit.ly/3ijvAqb

---

Nous avons essayé de livrer votre colis LP995215701FR, mais il n'y a aucun affranchissement. Suivez les instructions ici: http://bit.do/fHXvw

---

INFO ANTAI: Veuillez régulariser votre procès-verbal réalisé sous forme numérique de 35 EUR, REF: PV27AR23 via: https://mesamendes-antai2023.fr

---

De : L'Europe Brigade Nationale <cirparis.gendarmerieminister@gmail.com>
Envoyé : mardi 7 décembre 2021 12:37
À : gendarmerieparis@gouv.fr <gendarmerieparis@gouv.fr>
Objet : Rappel: DOSSIER N°322441

DIRECTION GÉNÉRALE DE LA GENDARMERIE

DIRECTION DE PROTECTION DES MINEURES

À votre attention :

CONVOCATION EN JUSTICE

Pour les nécessités d'une enquête judiciaire
(Article 390-1 du Code de procédure pénale)

Je suis M. Christian RODRIGUEZ, directeur général de la gendarmerie nationale en collaboration avec L'Office Européen De Police (Europol). Je vous contacte peu après une saisie informatique de cyber-infiltration (Autorisée, notamment en matière de pédopornographie, Site Pornographique, Cyber pornographie, pour vous informer que vous avez fait l'objet de plusieurs poursuites judiciaires en vigueur :

* LA PÉDOPORNOGRAPHIE
* SITE PORNOGRAPHIQUE
* CYBERPORNOGRAPHIE
* DÉTOURNEMENT DE MINEURS

Vous êtes prié de faire entendre par mail en nous écrivant vos justifications afin qu'elles soient mises en examen et vérifiées de sorte à évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport à Mme Maryvonne CAILLIBOTTE, procureur adjoint de la République près le tribunal de grande instance de Versailles et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, et vous serez fiché comme délinquant sexuel.

Votre dossier sera également transmis aux médias pour une diffusion où votre famille, vos proches et toute l'Europe entière verront ce que vous avez fait devant votre ordinateur.

Maintenant vous êtes averti.

Cordialement,

Glé. Christian RODRIGUEZ,
directeur général de la gendarmerie nationale.

DIRECTION CENTRALE DE LA GENDARMERIE
BRIGADE DE PROTECTION DES MINEURS
Adresse : 4 rue Claude-Bernard 92130 Issy-les-Moulineaux

----- Message transféré -----
De : "L'Agence Nationale des Traitements Automatisés des Infractions" <info@reaxium.com>

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANTAI
Agence Nationale de Traitement Automatisé des Infractions

Avis de contravention : 20240023879

Cher Conducteur,

Nous vous informons que vous avez une amende impayée pour non-respect des règles de stationnement payant, pour laquelle vous êtes redevable d'une amende de 35.00 €

Nous tenons à vous rappeler que la date limite de paiement de cette amende est [illegible] cette date, le montant de l[illegible].

URL d'origine :
https://redirection-online.com/
Cliquez ou appuyez pour suivre le lien.

CONSULTER

Ce site est entièrement sécurisé.

Nous vous invitons à régulariser votre situation dans les plus brefs délais.

© Direction générale des Finances publiques.

07 | GESTION DE CRISE

Je fais face à un incident,
JE CONTACTE :

et/ou

CRIC

www.campuscyber-na.fr/signaler-incident

0805.2929.40 (appel gratuit)

Vous apporte une **réponse technique**

Ouvre un incident au CRIC

CRC24 CENTRE DE RESSOURCES CYBERSÉCURITÉ

contact@crc.dordogne.fr
05.53.06.65.65

Vous indiquent les **1ers réflexes à adopter**

Parallèlement le CRC24 vous accompagne pour

- Contacter la Gendarmerie/Police
- Déposer une pré-Plainte en ligne
- Contacter le DPD (Délégué à la Protection des Données)


CRC 24
CENTRE DE RESSOURCES
CYBERSÉCURITÉ