



Livret Pédagogique



Formation Réalité Virtuelle Les Fondamentaux de la Cybersécurité



Société Aëlvir

Table des MATIÈRES



Introduction	3
Notre approche	4
Cyberspace, SI & IoT	5
La Cybersécurité, c'est quoi ?	6
Menaces & Risques Opérationnels	7
Sécurisation Physique	8
Réagir à une attaque	9
Accès sécurisés	10
Authentification forte	11
Hygiène Numérique	12
Hygiène Numérique (suite)	13
Point de vigilance VR	14
Ressources utiles	15
Lexique	16
Notes Personnelles	17
Contacts	18

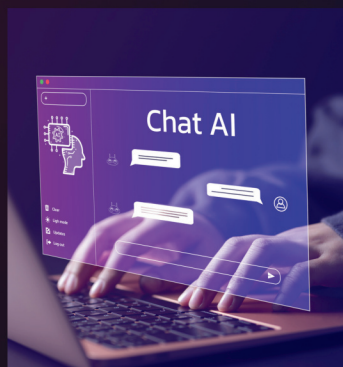
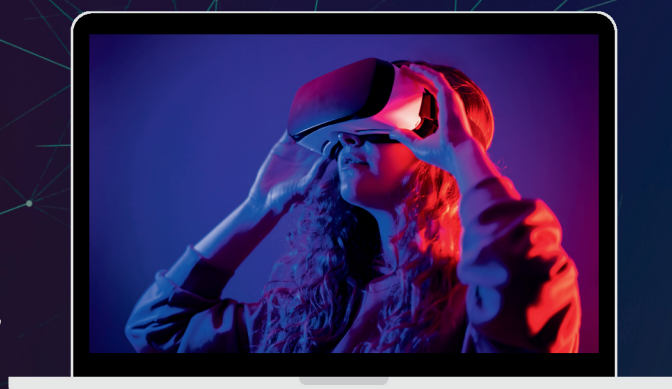


INTRODUCTION



COMMENT LA RÉALITÉ VIRTUELLE OUVRE LA VOIE À LA PÉRENNITÉ

La réalité virtuelle (RV) révolutionne l'apprentissage durable en créant des environnements immersifs qui favorisent un ancrage mémoriel profond. Elle améliore les compétences et renforce la mémoire à long terme, permettant une meilleure visualisation et pratique des concepts appris.



L'ANCRAGE MÉMORIEL AU CENTRE DE LA FORMATION

C'est un processus cognitif qui fixe les informations dans la mémoire à long terme. En associant de nouvelles connaissances à des concepts existants ou en utilisant des méthodes interactives, il facilite une meilleure rétention des informations.

REPLONGEZ-VOUS DANS L'EXPÉRIENCE

Vous trouverez ici une synthèse détaillée des notions abordées lors de votre formation en réalité virtuelle, des conseils concrets, des exemples, ainsi que des outils pour renforcer votre vigilance au quotidien.

NOTRE APPROCHE



Immersion en
réalité
virtuelle
réaliste

Formation façon
gaming pour une
simulation efficace

Apprentissage
actif donc
durable

Feedback
instantanés &
personnalisés
de votre
parcours

Répétition
illimitée des
tests, SANS
risque

Ancrage
mémoirel
renforcé

CYBERESPACE, SI & IOT



Les systèmes d'information (SI) et l'Internet des Objets (IoT) constituent ensemble le cyberspace !



Rappelez-vous !



C'est quoi tout ça ?

1 Cyberspace : Ce terme fait référence à l'environnement virtuel créé par les réseaux informatiques. Il englobe tous les systèmes interconnectés qui permettent le stockage, la modification et l'échange de données numériques.

2 Système d'Information (SI) : C'est l'ensemble des ressources (matériel, logiciel, données, procédures) permettant de collecter, stocker, traiter et diffuser l'information dans une organisation.

Pourquoi le SI est-il stratégique ?

- Il supporte toutes les **fonctions** de l'entreprise
- Il contient des données **sensibles** (clients, finances, projets, RH...).
- Sa compromission peut avoir des conséquences **graves** : arrêt de production, fuite de données, atteinte à la réputation

3 Internet des Objets (IoT) : Objets connectés capables d'envoyer/recevoir des données (caméras, imprimantes, capteurs...).

Risques

- Ports d'entrée peu protégés
- Mises à jour négligées

Exemples

- Caméra IP piratée
- Badge copié
- Imprimante utilisée comme passerelle d'infection

LA CYBERSÉCURITÉ C'EST QUOI ?

Ensemble des pratiques, outils et réflexes visant à protéger les systèmes, réseaux et données contre les attaques, vols ou destructions !



Rappelez-vous !

Clients à contacter :

- Argent*
- Victor Porte : 06.06.06.06.06
 - Laura Bougle : 07.07.07.07.07
 - Steve Normand :
steve.normand@cywiz.fr
 - Eva Nésense :
contact@eva-sav.com

Pourquoi c'est essentiel aujourd'hui ?

- 1 Explosion des attaques (ransomware, phishing, Hameçonnage ciblé, Injections SQL, Attaques DoS & DDos, Malware, etc...)
- 2 Multiplication des appareils connectés.
- 3 Conséquences graves : pertes financières, arrêt d'activité, fuite de données, réputation

Exemples d'incidents concrets

- 1 Ransomware : Une entreprise paralysée, rançon exigée pour débloquer les données
- 2 Phishing : Un collaborateur clique sur un faux mail, ses identifiants sont volés.
- 3 Fuite de données : Un mot de passe noté sur un post-it, retrouvé par un visiteur, des informations sensibles sur un bloc-notes...

Qui est concerné ?

- 1 Entreprises et institutions : Sécurité des systèmes et des données.
- 2 Utilisateurs individuels : Pour protéger leurs informations personnelles.
- 3 Gouvernements : Pour défendre les infrastructures critiques et les données sensibles.

MENACES & RISQUES OPÉRATIONNELS



Connaître les menaces et mécanismes d'attaque en constante évolution permet d'évaluer les risques et de concevoir des stratégies de défense efficaces pour sécuriser systèmes et données.



Les Principales Menaces

Aujourd'hui, entreprises, institutions et gouvernements font face à des cybermenaces sophistiquées comme les rançongiciels et le phishing, exploitant les failles des systèmes et les erreurs humaines.

La cybersécurité est essentielle. Pour se protéger, les organisations doivent adopter une approche proactive avec des mesures de protection solides & la formation constante des employés. En comprenant les risques et en appliquant des stratégies de défense efficaces, elles peuvent mieux se défendre contre les cyberattaques et protéger leurs actifs numériques.



Les mécanismes d'attaques

Les mécanismes d'attaque en cybersécurité sont les méthodes utilisées par les cybercriminels pour exploiter les failles des systèmes. Quelques exemples :

- Exploitation de **failles** (logiciels obsolètes, mots de passe faibles)
- Vecteurs : **clé USB** piégée, email, site web frauduleux
- Accès physique **négligé** (PC non verrouillé, badge traînant)

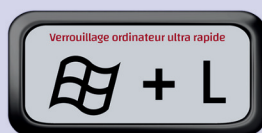
- Hameçonnage ("Phishing")
- Piratage de compte
- Faux support Technique
- Virus
- Violation de données
- Piratage informatique
- Ingénierie sociale
- Rançongiciels (ransomwares)
- Faux ordre de virement
- Attaque en Déni de Service
- Défiguration site internet

SÉCURISATION PHYSIQUE

La sécurisation physique en matière de cybersécurité fait référence aux mesures prises pour protéger les systèmes informatiques, les réseaux et les données contre les accès physiques non autorisés ou les dommages. Cela inclut la protection des équipements matériels tels que les serveurs, les routeurs, les câbles, ainsi que les dispositifs de stockage de données.



Rappelez-vous !



Sous macOS

Cmd + Maj + Q

Sécurisation physique




- 1** **Contrôle d'accès** : Utilisation de badges, de cartes d'accès, de biométrie ou de codes PIN pour limiter l'accès aux zones sensibles
- 2** **Verrouillage des postes de travail** : Verrouillez toujours votre ordinateur en appuyant sur **Windows + L** lorsque vous vous absentez !
- 3** **Surveillance** : Installation de caméras de surveillance pour surveiller les zones critiques et décourager les intrusions
- 4** **Verrouillage des équipements** : Utilisation de serrures et de boîtiers sécurisés pour protéger les équipements contre le vol ou la manipulation.
- 5** **Gestion des visiteurs** : Procédures strictes pour l'enregistrement et l'accompagnement des visiteurs dans les zones sensibles.
- 6** **Sécurité des bureaux et des salles de serveurs** : Les zones contenant des équipements informatiques doivent être verrouillées et accessibles uniquement au personnel autorisé.
- 7** **Protection des appareils mobiles** : Les PC, portables, tablettes et smartphones doivent être sécurisés avec des MDP ou des méthodes d'authentification biométrique. Ils doivent aussi être protégés contre le vol ou la perte.
- 8** **Sécurité des câbles** : Protection des câbles réseau et des fibres optiques contre les coupures ou les écoutes clandestines

RÉAGIR A UNE ATTAQUE

Face à une cyberattaque, une réaction efficace est essentielle pour limiter les dégâts, protéger les données et préserver la confiance. Une réponse rapide et structurée réduit les impacts financiers et opérationnels, tout en sauvegardant la réputation de l'organisation.





Signes à détecter

-  Ordinateur lent, fichiers inaccessibles
-  Apparition de messages anormaux
-  Activité réseau inhabituelle

Réflexes immédiats

- 1 Déconnecter l'appareil du Réseau !
NE PAS DÉBRANCHER VOS APPAREILS !!
- 2 Prévenir le référent sécurité
- 3 Ne pas effacer les preuves
- 4 Documenter ce que vous avez vu
- 5 Informer immédiatement les parties prenantes & les autorités compétentes

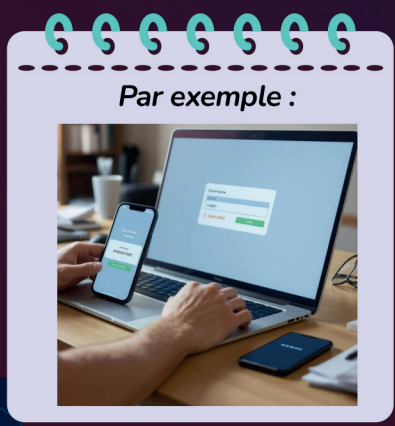
Obligations légales

-  Fuite de données ? : déclaration CNIL sous 72h (RGPD)
-  Chacun est responsable de la sécurité de ses accès



ACCÈS SÉCURISÉS

La sécurisation des accès est un pilier fondamental de la cybersécurité moderne, visant à protéger les systèmes d'information contre les accès non autorisés et les menaces potentielles. Ce poste est la plupart du temps assuré par le DSI ou le responsable Informatique.



Par exemple :

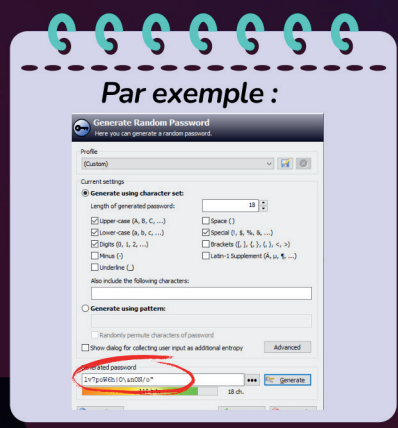
Sécurisation des Accès

- 1 Authentification Multifactor (MFA) :** Utilisation de deux ou plusieurs méthodes d'authentification pour vérifier l'identité d'un utilisateur. Par exemple, un mot de passe combiné avec un code envoyé par SMS ou une empreinte digitale.
- 2 Gestion des Identités et des Accès (IAM) :** Systèmes qui gèrent les identités numériques et les droits d'accès des utilisateurs. Cela inclut la création, la modification et la suppression des comptes utilisateurs et des permissions.
- 3 Chiffrement des Données :** Protection des données sensibles en les rendant illisibles sans une clé de déchiffrement. Cela peut être appliqué aux données en transit (par exemple, via SSL/TLS) et aux données au repos.
- 4 Réseaux Privés Virtuels (VPN) :** Permettent aux utilisateurs d'accéder de manière sécurisée à un réseau privé via Internet, en chiffrant les communications pour protéger les données.
- 5 Contrôle d'Accès Basé sur les Rôles (RBAC) :** Attribution des permissions en fonction des rôles des utilisateurs au sein de l'organisation, limitant l'accès aux ressources nécessaires pour leurs fonctions.

AUTHENTIFICATION FORTE



L'authentification forte, ou authentification multifacteur (MFA), est une méthode de sécurité essentielle qui exige deux formes de vérification ou plus pour accéder aux systèmes et données sensibles, renforçant ainsi la sécurité par rapport aux simples mots de passe.



Méthodes

- 1** **Quelque chose que vous savez** : mots de passe, codes PIN ou les réponses à des questions secrètes. Bien que couramment utilisés, ces éléments doivent être combinés avec d'autres facteurs pour être considérés comme une authentification forte.
- 2** **Quelque chose que vous avez** : Cela peut être un objet physique comme une carte à puce, un jeton de sécurité (token), ou un appareil mobile qui reçoit des codes de vérification par SMS ou via une application d'authentification.
- 3** **Quelque chose que vous êtes** : Cela fait référence aux caractéristiques biométriques, telles que les empreintes digitales, la reconnaissance faciale/vocale ou le scan de l'iris.



Créer un mot de passe sécurisé

- **Longueur** : 12 caractères minimum
- **Mélanger** lettres, chiffres, symboles
- Ne **jamais** partager ni réutiliser un mot de passe
- Utiliser un **gestionnaire** de mots de passe
- Changez vos MDP tous les 3 à 6 mois
- N'**envoyez** JAMAIS vos mots de passe par e-mail ou par téléphone
- Conformez-vous aux règles instaurées par votre entreprise/institution

HYGIÈNE NUMÉRIQUE

8 Cyber Réflexes pour se protéger sur Internet



1

Utiliser des Mots de Passe Forts

Un mot de passe fort est essentiel pour sécuriser vos comptes en ligne contre les accès non autorisés. Évitez les mots de passe simples, les informations personnelles (comme votre date de naissance) ou les séquences évidentes, qui sont facilement devinées par des attaques automatisées.

Bonnes Pratiques

Un mot de passe idéal est long (12 caractères minimum), unique, complexe (mélanger lettres, chiffres, symboles), mis à jour régulièrement, jamais réutilisé, géré via un gestionnaire sécurisé

2

Authentification à 2 Facteurs

L'authentification à deux facteurs ajoute une couche supplémentaire de sécurité en demandant une deuxième vérification, généralement un code envoyé par SMS ou généré par une application

Bonnes Pratiques

L'authentification à 2 facteurs (A2F) enforce la sécurité en exigeant un mot de passe et un code unique via SMS, e-mail, application ou clé physique.

3

Mettre à Jour les Logiciels

Les mises à jour corrigent des failles de sécurité exploitables par des cyberattaques pour accéder à vos données ou contrôler vos appareils. Ignorer ces mises à jour augmente le risque de vulnérabilités, laissant votre système exposé aux virus, ransomwares et autres logiciels malveillants.

Bonnes Pratiques

Inventoriez les appareils, activez les mises à jour automatiques (après sauvegarde), testez-les, utilisez des outils centralisés, définissez une politique de mise à jour, automatisez avec des logiciels sécurisés, et restez vigilant(e) aux alertes.

4

Se Méfier des Liens et PJ

Les liens et pièces jointes peuvent contenir des virus ou logiciels malveillants visant à voler vos données ou infecter vos appareils. En entreprise, n'utilisez pas votre messagerie personnelle et limitez-vous aux outils de communication professionnels

Bonnes Pratiques

Ne cliquez pas sur des liens ou pièces jointes d'expéditeurs inconnus. Vérifiez l'authenticité des messages en examinant l'adresse de l'expéditeur, les fautes, et soyez attentif aux demandes urgentes ou pièces jointes inattendues.

HYGIÈNE NUMÉRIQUE (SUITE)



8 Cyber Réflexes pour se protéger sur Internet

5

Antivirus et un Pare-feu

Un antivirus et un pare-feu sont essentiels pour vous protéger contre les logiciels malveillants, les tentatives d'intrusion et le vol de données. L'antivirus détecte et neutralise les fichiers suspects, tandis que le pare-feu surveille et filtre les connexions réseau, bloquant les accès non autorisés à vos appareils.

Bonnes Pratiques

Installez un antivirus officiel, activez un pare-feu, utilisez les outils de sécurité de l'entreprise, respectez les politiques d'accès réseau et signalez toute activité suspecte.

6

Surfer en Mode Sécurisé

Utiliser des connexions sécurisées (HTTPS) protège vos données en chiffrant les informations échangées, ce qui est crucial sur les réseaux publics où les risques de piratage et d'espionnage sont élevés. Assurez-vous que le cadenas soit visible dans la barre d'adresse avant de transmettre des informations sensibles.

Bonnes Pratiques

Vérifiez que l'URL commence par 'https://' avant de saisir des informations personnelles. Attention aux réseaux Wi-Fi publics, souvent non sécurisés ; utilisez un VPN.

7

Sécurisation & Gestion des accès

La sécurisation des accès se concentre sur la gestion et le contrôle des permissions d'accès aux systèmes d'information et aux données. Elle implique l'utilisation de politiques de sécurité robustes, de gestion des identités et des accès (IAM), et de technologies de chiffrement pour protéger les informations sensibles.

Bonnes Pratiques

Appliquez le principe du moindre privilège et supprimez les comptes inutilisés !

8

Sécurisation physique

La sécurisation physique protège les installations, équipements et personnes contre les accès non autorisés, les dommages ou les vols. Cela inclut badges d'accès, systèmes de surveillance, contrôles d'entrée et de sortie sécurisés, ainsi que des procédures de sécurité strictes.

Bonnes Pratiques

Verrouillez vos postes de travail même pour une courte absence !

Un geste rapide :

Touche Windows + L ou **Cmd + Ctrl + Q**

Contrôlez les accès aux locaux !

LES POINTS DE VIGILANCE EN VR



Dans la session en réalité virtuelle, vous avez été confronté (e) à 15 situations à risque. Voici le détail et les bonnes pratiques généralement associées.

Point de vigilance	Risque	Bonne pratique
Clé USB inconnue	Infection, vol de données	Utilisez uniquement des clés autorisées, signalez au responsable
Badge laissé sur le bureau	Intrusion, usurpation	Gardez-le sur vous, ne le prêtez jamais
Carte de visite oubliée	Usurpation d'identité	Rangez-les, détruisez les anciennes
Webcam non couverte	Espionnage	Utilisez un cache physique
Post-it avec MDP	Vol d'accès	Utilisez un gestionnaire, ne notez rien à vue
Téléphone non sécurisé	Accès non autorisé	Code, empreinte, verrouillage automatique
Ordinateur non verrouillé	Accès à vos données	Verrouillez dès que vous quittez le poste (w + L) ; (Cmd + Ctrl + Q)
Phishing/fraude au Président	Vol d'identifiants, ransomware, infections	Vérifiez l'expéditeur, ne cliquez pas sans vérifier
Mot de passe trop simple	Piratage, intrusion	Mot de passe complexe, unique
Site interdit sur tablette	Infection, fuite, risque législatif pour l'entreprise	Fermez la session, fuyez les sites non professionnels
Infos confidentielles tableau blanc	Fuite d'informations	Effacez systématiquement après usage
Imprimante en veille	Point d'accès non sécurisé au réseau	Mettre à jour les Firmware, bien configurer l'accès réseau
Alerte intrusion	Propagation de la malveillance sur le réseau	Coupez seulement le réseau pour isoler le malware
NAS porte ouverte	Accès non autorisé - Vol	Vérifiez, fermez & sécurisez l'accès physique
Serveur / carte bancaire	Vol de données, détournement financier	Sécurisez au maximum

RESSOURCES UTILES

Identifier les principaux organismes publics à contacter en cas d'incident de sécurité des données et comprendre les responsabilités légales de chacun.

ANSSI

Agence Nationale de la Sécurité des Systèmes d'Information

<https://cyber.gouv.fr/fr>

En cas d'incident
Contacter le CERT-FR

3218

17cyber.gouv.fr

- Rôle : Autorité nationale en matière de sécurité des systèmes d'information
- Responsabilités :
 - Assurer la sécurité des systèmes d'information des administrations et des opérateurs d'importance vitale (OIV).
 - Fournir des recommandations et des guides de bonnes pratiques en matière de cybersécurité.
 - Gérer les incidents de sécurité affectant les infrastructures critiques.

CNIL

Commission Nationale de l'Informatique et des Libertés

La CNIL doit être notifiée dans les 72 heures suivant la découverte d'une violation de données personnelles

<https://notifications.cnil.fr/notifications/index>

- Rôle : Autorité française de protection des données personnelles.
- Responsabilités :
 - Superviser l'application du RGPD en France.
 - Recevoir les notifications de violation de données.
 - Fournir des conseils et des recommandations sur la protection des données.
 - Enquêter sur les plaintes et imposer des sanctions en cas de non-conformité.

Gendarmerie / Police Nationale

Pour signaler les incidents de cybercriminalité : 1 seul N°

17

- Rôle : Forces de l'ordre responsables de la sécurité publique
- Responsabilités :
 - Enquêter sur les cybercrimes et les violations de données.
 - Collaborer avec d'autres organismes pour lutter contre la cybercriminalité.

LEXIQUE

La cybersécurité est essentielle pour protéger les informations et les systèmes contre les attaques. Connaître les principaux termes de son lexique permet aux employés d'identifier les menaces et d'adopter des pratiques de sécurité solides, cruciales pour protéger les données personnelles et celles de l'entreprise. Voici quelques termes clés à connaître .



MALWARE	Logiciel malveillant conçu pour endommager, exploiter ou obtenir un accès non autorisé à un système informatique
PHISHING (Hameçonnage)	Technique d'escroquerie où l'attaquant usurpe une identité de confiance pour obtenir des informations sensibles.
RANSOMWARE	Logiciel malveillant qui chiffre les données d'une victime et exige une rançon pour les restaurer
VIRUS	Programme malveillant qui se réplique en s'insérant dans d'autres programmes ou fichiers, causant des dommages ou des perturbations.
MFA Authentif. Multifacteur	Système de sécurité nécessitant plusieurs vérifications pour l'accès à un compte.
CHIFFREMENT	Processus de conversion de données en un code pour empêcher l'accès non autorisé, assurant ainsi la confidentialité et la sécurité des informations
PARE-FEU (FIREWALL)	Système de sécurité surveillant et contrôlant le trafic réseau selon des règles prédéfinies pour bloquer les accès non autorisés.
Ingénierie Sociale	Technique manipulant les individus pour divulguer des informations confidentielles ou effectuer des actions compromettantes
ZERO-DAY	Faible inconnue exploitable avant qu'un correctif ne soit disponible
BOTNET	éseau de dispositifs infectés contrôlés à distance pour des activités illicites, comme des attaques DDoS ou l'envoi de spam
SECURITE DES RESEAUX	La sécurité des réseaux protège l'intégrité, la confidentialité et la disponibilité des données contre les accès non autorisés et les attaques
VPN Virtual Private Network)	Service qui sécurise et anonymise la connexion Internet
HACK	Intrusion non autorisée dans un système informatique pour exploiter ou compromettre ses fonctionnalités ou ses données
PATCH	Mise à jour logicielle conçue pour corriger des bugs, des failles de sécurité ou améliorer les fonctionnalités d'un programme

NOTES PERSONNELLES

Utiliser cette page pour noter les points clés, vos réflexions ou vos questions après la formation, en veillant à ne rien écrire de confidentiel.



A large rectangular area with horizontal blue lines, intended for taking personal notes.

CONTACTS



Besoin d'un renseignement supplémentaire sur votre expérience Cybersécurité en réalité virtuelle, nous contacter dans un premier temps par mail à l'adresse suivante :

contact@cywiz.fr

