

Mon Collège.

Prise en main d'un poste de travail numérique du Collège.

Observation, Découverte, Investigation, Résolution



5^{eme} - Activité 1

Compétences développées Technologie : 1.1.4, 1.1.6, 1.1.5 (Pix : 2.1)

I. Création, enregistrement puis impression de votre page de garde.

Vous devez vous connecter au réseau du collège puis créer votre dossier de technologie « Techno5 » dans l'espace « Documents ».

Après avoir effectué un « Copier/Coller » du raccourci d'accès « Site-Techno » à votre site de technologie, télécharger la page de garde de votre classeur.

Cette page, une fois complétée (nom, prénom, classe) sera sauvegardée dans votre dossier « Techno5 »

Ressource à votre disposition : un dossier d'aide.

II. Observer ces illustrations.

Source : Édition Nathan



DOC 1 Situation 1



DOC 2 Situation 2



DOC 3 Situation 3



DOC 4 Situation 4

a) Associer chaque situation au phénomène qu'elle illustre en indiquant son numéro.

- Atteinte à la vie privée : situation	- Stockage de fichiers mal organisé : situation
- Usurpation d'identité : situation	- Cyberharcèlement : situation

b) Citer un autre phénomène qui n'est pas illustré et qui représente un impact négatif du numérique sur la vie privée.

.....

III. Avoir une approche sécurisée lorsque vous utilisez un système numérique.

Nous vous proposons de faire un test qui caractérise vos usages en termes de protection de données. Si votre score est 20, vous avez une pratique sécurisée du numérique. S'il se rapproche de 0, alors il va falloir faire évoluer vos pratiques en reprenant les questions.



Entourez les chiffres des colonnes « Oui » ou « Non » selon votre situation et **calculez** votre score en les additionnant.

Score :

Questions	Oui	Non	Pour votre information
a) Êtes-vous inscrit sur un réseau social (TikTok, YouTube, WhatsApp, Instagram...)?	2	0	La loi du 7 juillet 2023 instaure une majorité numérique à 15 ans . Il est illégal de s'inscrire seul sur un réseau social avant 15 ans.
b) Avez-vous un mot de passe différent pour chacune de vos applications ?	3	0	Utiliser des mots de passe différents selon les applications permet de se protéger contre le piratage , notamment si l'un d'entre eux a été découvert.
c) Changez-vous vos mots de passe tous les 6 mois ?	3	0	Changer régulièrement de mots de passe permet de limiter les risques de se faire pirater.
d) Vos mots de passe sont-ils composés d'un minimum de 10 caractères incluant au moins une majuscule, une minuscule, un chiffre et un symbole ?	2	0	Il est fortement conseillé d'utiliser des mots de passe qui sont difficiles à trouver. Utiliser un mot de passe composé de chiffres et de symboles renforce la sécurité.
e) Vos applications (ex. : Word ou Explorer) et vos systèmes d'exploitation (ex. : Windows ou macOS, Android) sont-ils mis à jour automatiquement ?	2	0	Les logiciels sont mis à jour régulièrement afin de combler des problèmes de sécurité.
f) Avez-vous paramétré l'appareil photo de votre téléphone pour supprimer la localisation ?	2	0	Le téléphone stocke énormément d'informations dans une photo (heure, date, coordonnées GPS...). Lorsqu'on envoie une photo, on transfère également ces informations. Ce sont les données EXIF . Il existe des méthodes pour toutes les supprimer.
g) Savez-vous reconnaître le <i>phishing</i> ?	2	0	L'hameçonnage ou <i>phishing</i> est une forme d'escroquerie sur Internet . Le fraudeur se fait passer pour un organisme que vous connaissez et vous demande de cliquer sur un lien qui va récupérer vos données (photos, contacts, mots de passe...). Si vous en êtes victime, signalez-le sur www.internet-signalement.gouv.fr
h) Lisez-vous le type de données que vous partagez avant de cliquer sur « Accepter » lors de l'installation d'une application ?	2	0	Certaines de ces applications peuvent être conçues pour collecter secrètement des données personnelles, diffuser des publicités intrusives...
i) Avez-vous un antivirus sur votre ordinateur ?	2	0	L'utilisation d'un logiciel antivirus permet de se prémunir de certaines attaques numériques.