Cas courant d'usurpation d'identité sur un espace numérique de travail

1 L'usager (élève, parent, personnel) télécharge ou installe un logiciel ou une extension depuis une source non fiable (site non officiel, réseaux sociaux, site contrefait).

2 Le logiciel ou l'extension installé contient un système malveillant dérobeur de mot de passe ("stealer"), qui transmet au pirate informatique tous les identifiants et mots de passe enregistrés sur le navigateur.

3 Le pirate informatique peut usurper le compte de la victime grâce aux identifiants dérobés, ou revendre ses identifiants.

Une personne malveillante peut alors envoyer des messages à la place de la victime.

En réinitialisant tous les mots de passe, le pirate informatique ne peut plus se connecter sur les comptes de la victime.

Adopter des gestes simples pour sécuriser ses pratiques numériques

Télécharger des logiciels uniquement depuis une source fiable, en s'assurant d'avoir un antivirus actif et à jour sur tous vos équipements numériques.

Utiliser un mot de passe différent sur chaque site, de 12 signes minimum, mélangeant majuscules, minuscules, chiffres et caractères spéciaux.

Privilégier l'utilisation d'un gestionnaire de mots de passe et ne les communiquer à personne.

Région académique Occitanie
CC BY NC SA