

Restez en sécurité dans le cloud

Protégez toujours vos comptes avec des mots de passe robustes et utilisez des mots de passe différents pour chaque service cloud.

#StoppaCyberto

play.google.com

p1ay.go0gel.exe



Navigation Internet sécurisée

Assurez-vous d'être bien sur le site web que vous souhaitez visiter en vérifiant le domaine ou en utilisant un moteur de recherche pour trouver la version officielle du site.

#StoppaCyberto



Protégez vos appareils

Ne laissez pas vos appareils mobiles sans surveillance dans les lieux publics et assurez-vous que vos systèmes d'exploitation sont à jour.

#StoppaCyberto



Ne vous laissez pas piéger par les arnaques par hameçonnage !

Méfiez-vous des courriels qui tentent de créer un sentiment d'urgence, par exemple en demandant un paiement immédiat ou le téléchargement d'une pièce jointe.

#StoppaCyberto



N'oubliez pas la sécurité physique.

Ne laissez jamais de documents confidentiels sans surveillance, par exemple dans la corbeille de l'imprimante ou sur votre bureau.

#StoppaCyberto



Soyez prudent lorsque vous utilisez des réseaux Wi-Fi publics.

Assurez-vous de ne vous connecter qu'à des réseaux légitimes en vérifiant attentivement le nom du réseau.

#StoppaCyberto



Protégez vos supports amovibles

Rangez toujours vos supports amovibles dans une armoire sécurisée lorsqu'ils ne sont pas utilisés.

#StoppaCyberto



Assurez-vous que votre mot de passe est sécurisé.

Vos mots de passe doivent être uniques,
privés et faciles à retenir pour vous, mais
difficiles à deviner pour les pirates
informatiques.

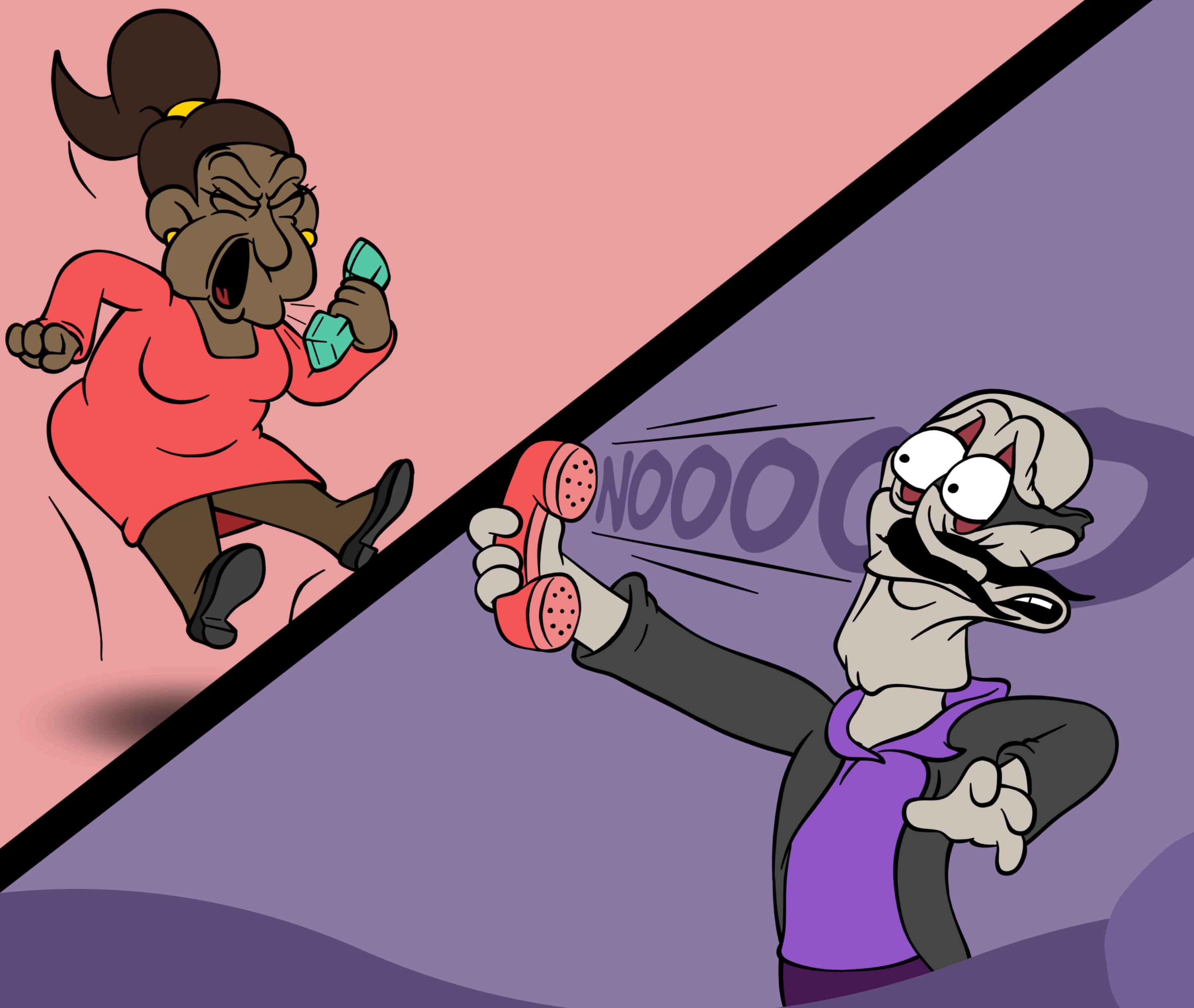
#StoppaCyberto



Soyez particulièrement vigilant(e) à votre sécurité lorsque

vous travaillez à domicile.
Changer le mot de passe par défaut de votre routeur domestique et mettre à jour son micrologiciel réduit le risque d'attaque par un pirate informatique.

#StoppaCyberto



Méfiez-vous de l'ingénierie sociale

Soyez prudent si l'on vous demande de faire quelque chose que vous ne feriez pas normalement (par exemple, envoyer de l'argent, installer quelque chose, partager des données client, etc.).

#StoppaCyberto



Soyez prudent sur les réseaux sociaux.

Limitez vos paramètres de confidentialité sur les réseaux sociaux et évitez de partager des informations sensibles qui pourraient être utilisées à mauvais escient par des

cybercriminels.
#StoppaCyberto