Matthieu Audibert **@GendAudibert** *Sun Mar 13 20:43:03 +0000 2022*

#Thread

Après plusieurs questions reçues, quelques conseils (orientés grand public) pour renforcer sa **#Cybers**écurité sur Twitter

L'idée est d'une part de protéger son compte et d'autre part de protéger sa vie privée.

1/18 ■■

1/ Protéger son compte

L'adresse email : il vaut mieux utiliser une adresse email dédiée à ce réseau social et non utilisée sur un autre réseau ou un magasin en ligne.

Objectif : limiter le risque de se faire avoir par un **#Phishing**

2/18 ■■

https://t.co/O6OTv2PCYi

Le mot de passe et l'authentification

Il est fortement recommandé d'utiliser un mot de passe complexe, unique et réservé à Twitter.

En outre et comme Twitter le propose, il faut activer l'authentification à deux facteurs

3/18 ■■

https://t.co/SHcUp3lvDK

Pour le 2nd facteur, je conseille une app sur le téléphone qui génère un code unique aléatoire

Objectif : si l'email et le mdp sont compromis, limiter au maximum le risque de piratage du compte et se prémunir d'un éventuel SIM Swapping

4/18■■

https://t.co/XNX8wPvdr2

Plusieurs applications d'authentification sont disponibles sur l'App Store et le Play Store.

Tapez authentification dans le moteur de recherche et choisissez celle qui vous convient.

5/18 ■■

https://t.co/Hl3NsKJKr0

Pour renforcer la sécurité de son compte, il est recommandé d'activer la protection de réinitialisation de votre mot de passe.

Objectif : éviter que quelqu'un déclenche un envoi massif de mails ou sms sur votre email ou votre téléphone

6/18■■

https://t.co/IvSHckap9b

Le choix du @

L'usage d'un pseudo est particulièrement recommandé si vous ne souhaitez pas afficher votre identité sur Twitter

C'est un choix libre qui protège par nature votre vie privée

Choisissez un @ dédié à Twitter et ne l'utilisez jamais sur un autre réseau social

7/18■■

Objectif : limiter au maximum la cartographie (le mapping) de votre vie numérique.

Si on tape votre @ dans Google ou un autre moteur de recherche, on ne doit pas tomber sur votre compte Instagram, Facebook ou Snapchat.

8/18■■

Dans le même ordre d'idée, si les pseudos sont différents, évitez de mettre dans votre description le lien vers un autre de vos comptes sur un réseau social.
Toujours le même objectif, éviter le mapping de votre vie numérique.
9/18■■

2/ Protéger sa vie privée
Que vous ayez choisi ou non un pseudo, soignez particulièrement vigilants aux points suivants : la géolocalisation des tweets.
10/18■■
https://t.co/71StcPxiSk

Si vous tweetez via une app sur votre téléphone, la localisation des tweets peut être extrêmement précise donc cela renseigne tout le monde sur votre position géographique, voir votre lieu d'habitation, votre lieu de travail, votre lieu d'étude, etc.
11/18■■

Les photos
Si vous êtes sous pseudo, ne mettez pas une photo de votre visage en PP.

Pourquoi ?
Avec une recherche inversée, il est très facile de vous retrouver sur Internet.
12/18■■

Idem, si vous mettez en ligne la photo d'une rue, d'un paysage ou d'un bâtiment, via quelques outils d' **#OSINT** il est très facile de retrouver le lieu où la photo a été prise.
13/18■■

Parfois le diable se cache dans les détails.
Les photos prises via un téléphone sont de très bonnes qualités, un éventuel attaquant peut travailler sur les reflets sur un miroir ou sur des lunettes de soleil..
14/18■■

Enfin, si votre compte est public (pas de cadenas), partez du principe que tout, absolument tout, ce que vous tweetez est public.
Votre famille peut le lire, votre employeur, votre enseignant, votre (ex) conjoint(e), etc.
15/18■■

Dernier conseil : limitez l'ouverture de vos DM. Accordez la possibilité de vous écrire en privé aux seules personnes que vous suivez.
16/18■■
https://t.co/uMRobZ4JrE

Conclusion
Ce sont des simples conseils orientés grand public. L'idée est que chacun(e) puisse renforcer sa **#cybers**écurité

Si vous rencontrez le moindre problème, n'hésitez pas à contacter **https://t.co/5vhug4vE3r** disponible 24h/24 et 7j/7
17/18■■
https://t.co/mZlQl64MPv

Enfin, si vous êtes victime de **#Cyberharc**èlement , vous pouvez vous reporter à ce thread
Fin.
18/18
https://t.co/Xl1DXEDNa6