Votre base de données avec des informations personnelles sera piratée

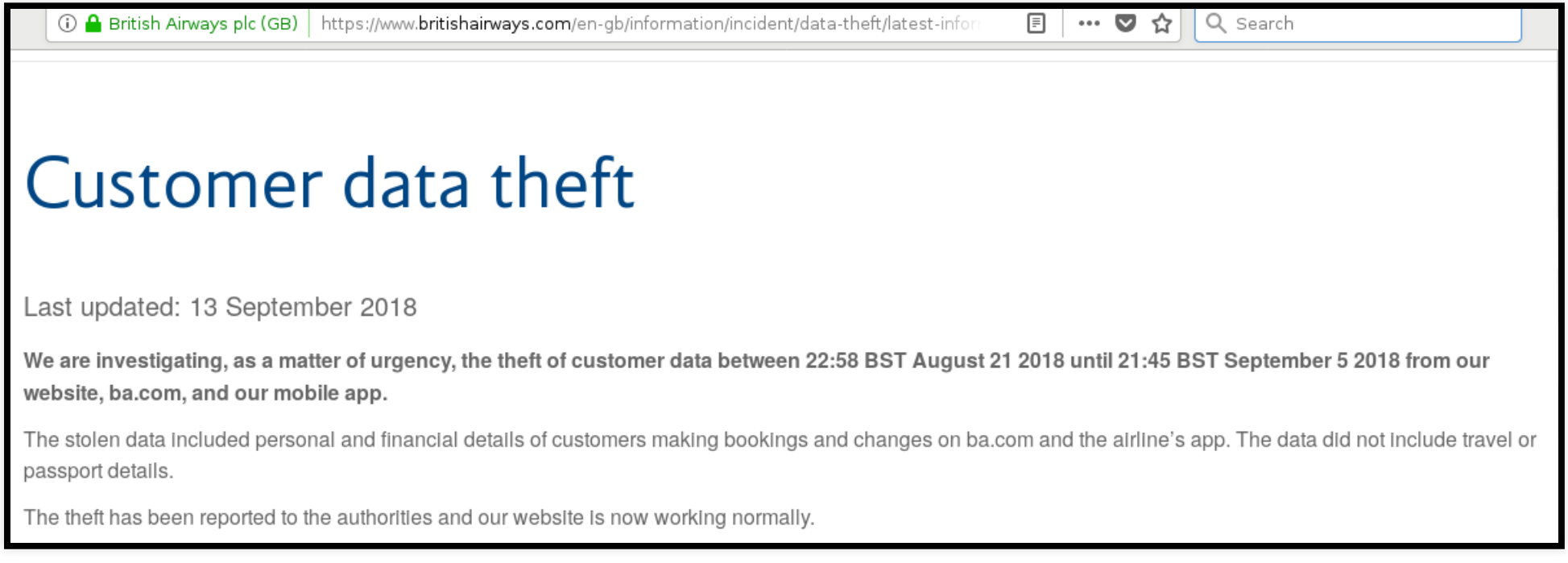
Paris Web, octobre 2018

Stéphane Bortzmeyer (AFNIC)
bortzmeyer+parisweb@nic.fr

Public visé

Cielles qui ont un site Web qui collecte des données personnelles (donc la plupart).
Rappel : les données sont personnelles même s'il n'y a pas le nom de la personne dedans.

British Airways



Vos données seront piratées un jour

Vos données seront piratées un jour

- Si, si.

Vos données seront piratées un jour

- Si, si.
- Sauf si vous êtes l'Indiana Jones ou la Lara Croft de la sécurité informatique

Vos données seront piratées un jour

- Si, si.
- Sauf si vous êtes l'Indiana Jones ou la Lara Croft de la sécurité informatique
- Sony, Equifax, l'Express et Yahoo ont été piratés, pourquoi pas toi ?

Vos données seront piratées un jour

- Si, si.
- Sauf si vous êtes l'Indiana Jones ou la Lara Croft de la sécurité informatique
- Sony, Equifax, l'Express et Yahoo ont été piratés, pourquoi pas toi ?
- Cela ne veut pas dire qu'il ne faut prendre aucune mesure de sécurité.

Vos données seront piratées un jour

- Si, si.
- Sauf si vous êtes l'Indiana Jones ou la Lara Croft de la sécurité informatique
- Sony, Equifax, l'Express et Yahoo ont été piratés, pourquoi pas toi ?
- Cela ne veut pas dire qu'il ne faut prendre aucune mesure de sécurité.
- Juste qu'il faut être conscient de ce qui arrivera, et s'y préparer.

Avant : faites comme toutes les autres boîtes

Avant : faites comme toutes les autres boîtes

1. Répétez bien fort : nous sommes sécurisés (vous pouvez aussi crier « anonymisés »),

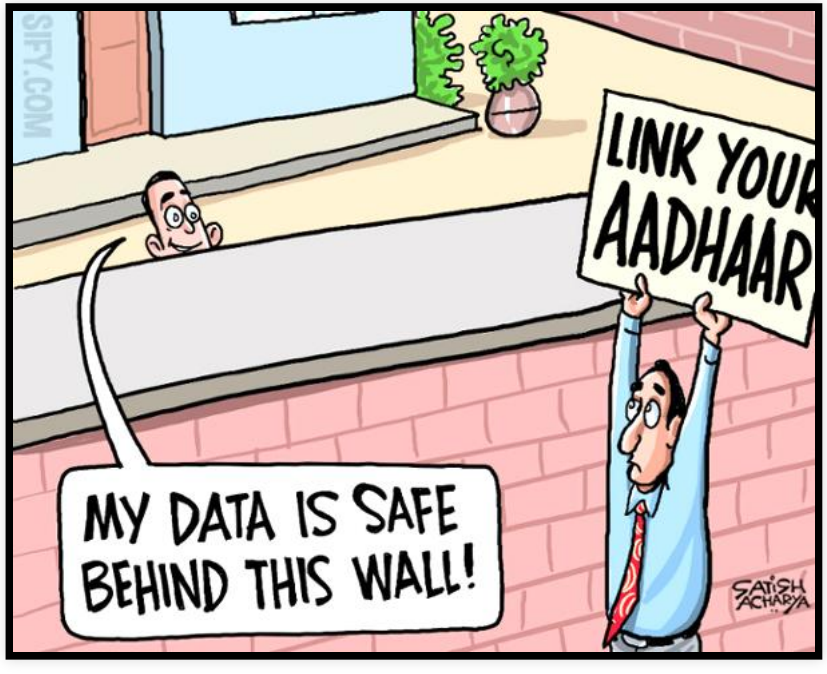
Avant : faites comme toutes les autres boîtes

1. Répétez bien fort : nous sommes sécurisés (vous pouvez aussi crier « anonymisés »),
2. Ajoutez quelques termes techniques : cryptage, 4 096 bits, *enterprise-grade* ou *military-grade*, citez des normes absconses,

Avant : faites comme toutes les autres boîtes

1. Répétez bien fort : nous sommes sécurisés (vous pouvez aussi crier « anonymisés »),
2. Ajoutez quelques termes techniques : cryptage, 4 096 bits, *enterprise-grade* ou *military-grade*, citez des normes absconses,
3. Bonus : évoquez un mur imprenable.

Aadhaar



Our data center has walls that are 13 feet high and 5 feet thickness.

(L'Attorney General, à propos de la base de données des citoyens indiens.)

Avant : les vrais recommandations

Minimisez les données !

Avant : les vrais recommandations

Minimisez les données !

1. Arrêtez de croire que le bonheur vient de la collecte massive,

Avant : les vrais recommandations

Minimisez les données !

1. Arrêtez de croire que le bonheur vient de la collecte massive,
2. Arrêtez de croire que les données sont « le pétrole du XXIe siècle » (sauf si vous travaillez pour Facebook),

Avant : les vrais recommandations

Minimisez les données !

1. Arrêtez de croire que le bonheur vient de la collecte massive,
2. Arrêtez de croire que les données sont « le pétrole du XXIe siècle » (sauf si vous travaillez pour Facebook),
3. Avez-vous **vraiment** besoin de cette information ? Exemple : si vous vous intéressez à l'âge des gens, pourquoi demander la date de naissance complète ?

Avant : les vrais recommandations

Minimisez les données !

1. Arrêtez de croire que le bonheur vient de la collecte massive,
2. Arrêtez de croire que les données sont « le pétrole du XXIe siècle » (sauf si vous travaillez pour Facebook),
3. Avez-vous **vraiment** besoin de cette information ? Exemple : si vous vous intéressez à l'âge des gens, pourquoi demander la date de naissance complète ?
4. C'est aussi une obligation légale (I&L puis RGPD).

Pendant : faites comme toutes les autres boîtes

Pendant : faites comme toutes les autres boîtes

1. Ignorez les signalements et les alertes,

Pendant : faites comme toutes les autres boîtes

1. Ignorez les signalements et les alertes,
2. Niez tout,

Pendant : faites comme toutes les autres boîtes

1. Ignorez les signalements et les alertes,
2. Niez tout,
3. Avouez finalement à contre-cœur la fuite, en la minimisant, quitte à mentir.

Pendant : faites comme toutes les autres boîtes

1. Ignorez les signalements et les alertes,
2. Niez tout,
3. Avouez finalement à contre-cœur la fuite, en la minimisant, quitte à mentir.

Toutes les entreprises citées plus haut ont procédé ainsi, pourquoi pas vous ?

Pendant : les vraies recommandations

En vrai, voici ce qu'il faudrait plutôt faire.

Faites circuler l'information en interne

Faites circuler l'information en interne

- Par exemple du CM aux informaticiens et vice-versa,

Faites circuler l'information en interne

- Par exemple du CM aux informaticiens et vice-versa,
- La plupart des entreprises cloisonnent au contraire,

Faites circuler l'information en interne

- Par exemple du CM aux informaticiens et vice-versa,
- La plupart des entreprises cloisonnent au contraire,
- D'où ces malheureux CM qui, sur Twitter, racontent n'importe quoi car eux-mêmes sont dans le noir.

Réagissez vite

Réagissez vite

- Le problème est **maintenant**, il n'y a pas forcément le temps de suivre les processus internes sacrés.

> *Aucun plan ne survit à la première rencontre avec l'ennemi.*

(Clausewitz)

Réagissez vite

- Le problème est **maintenant**, il n'y a pas forcément le temps de suivre les processus internes sacrés.

> *Aucun plan ne survit à la première rencontre avec l'ennemi.*

  (Clausewitz)

- Passez en mode crise : les règles classiques ne s'appliquent pas forcément.

Réagissez vite

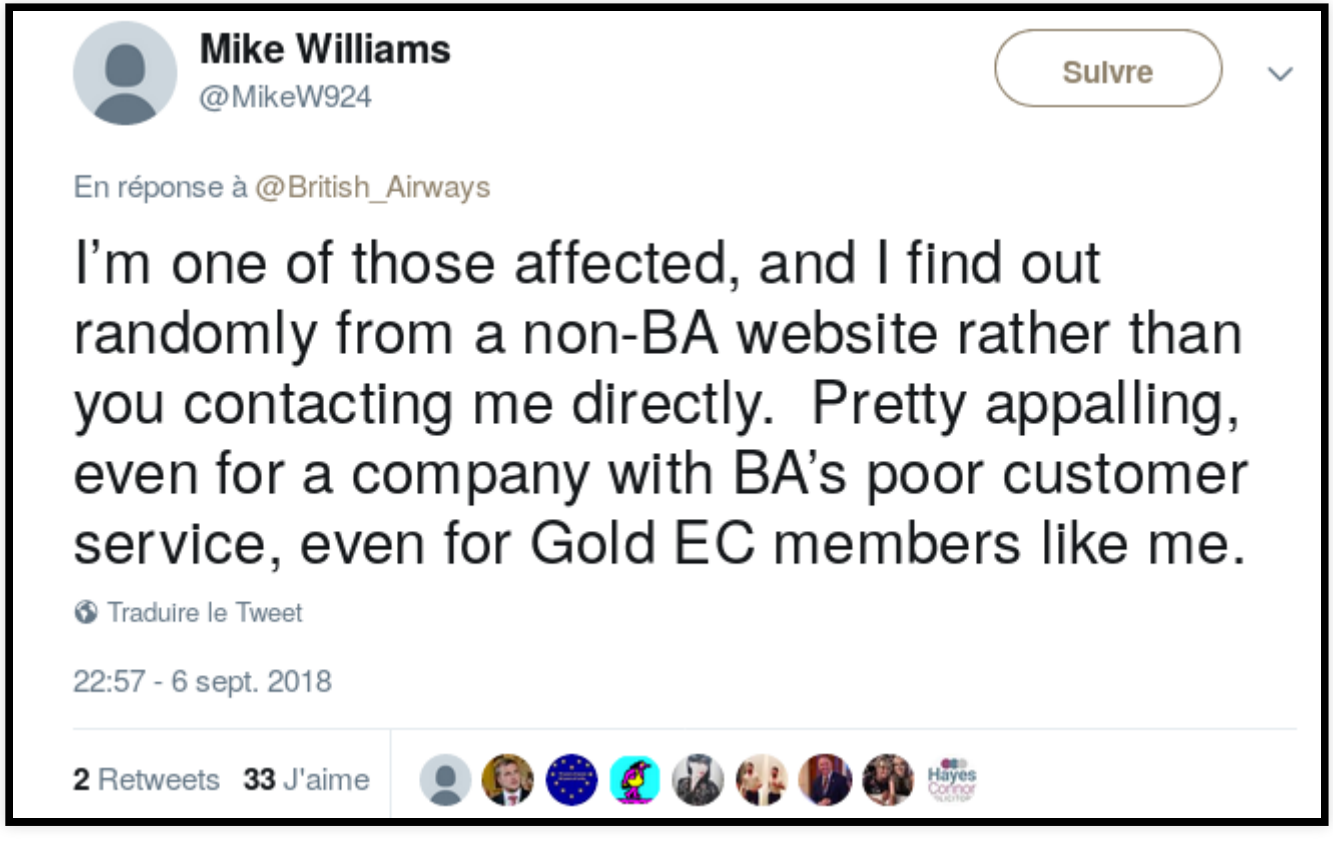
- Le problème est **maintenant**, il n'y a pas forcément le temps de suivre les processus internes sacrés.

> *Aucun plan ne survit à la première rencontre avec l'ennemi.*

(Clausewitz)

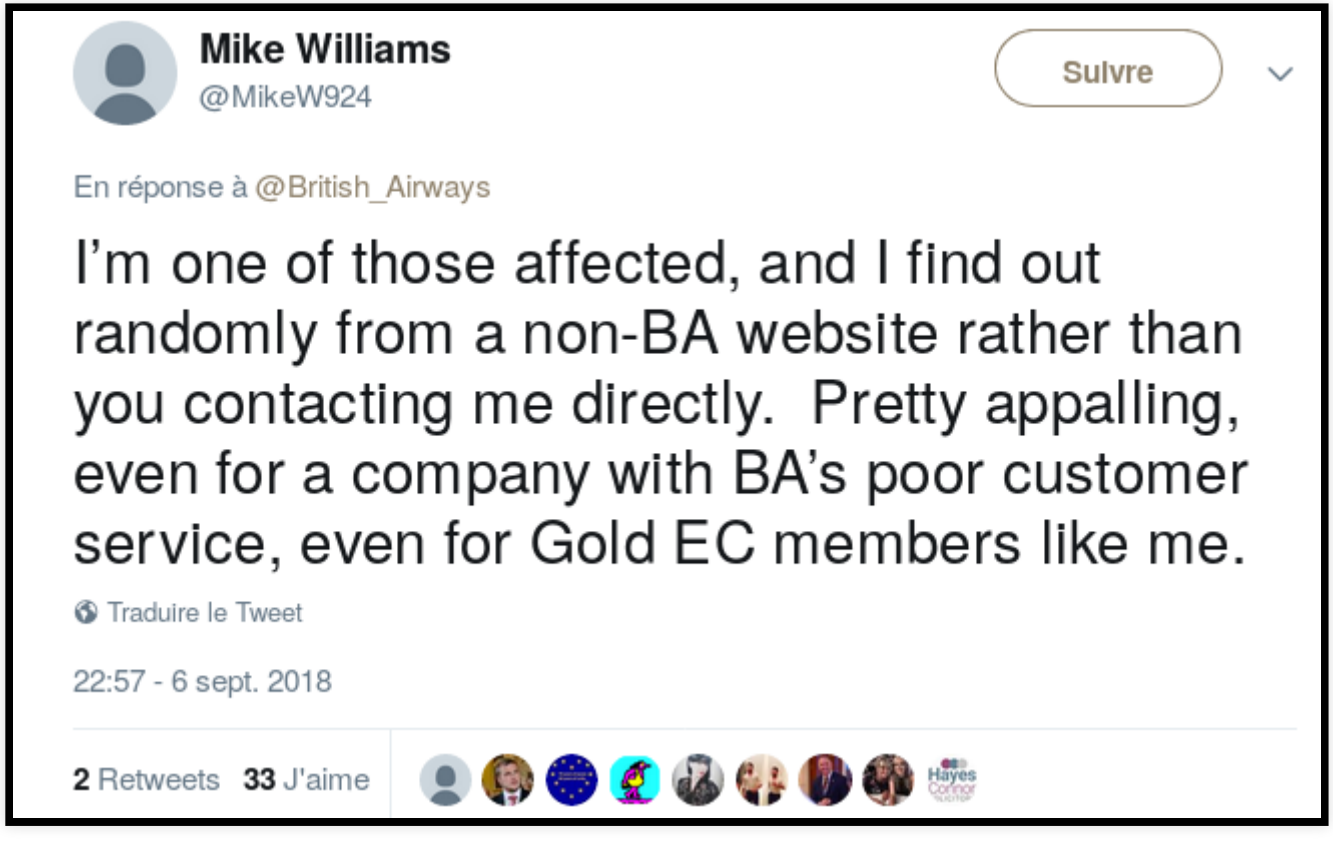
- Passez en mode crise : les règles classiques ne s'appliquent pas forcément.
- Mais réfléchissez quand même : une erreur est vite arrivée, dans la panique.

Prévenez les clients



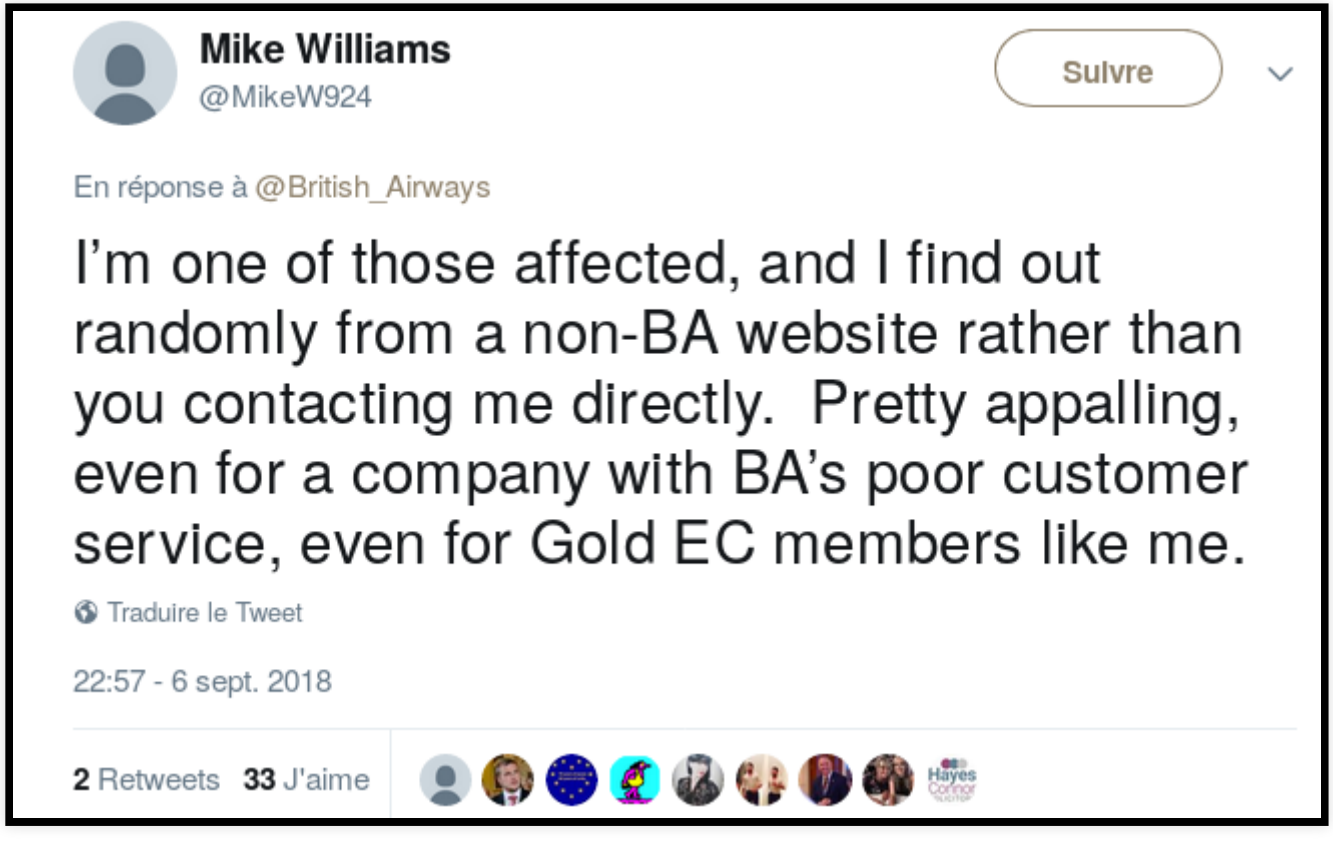
Prévenez les clients

- C'est d'ailleurs une obligation légale



Prévenez les clients

- C'est d'ailleurs une obligation légale
- *«Déterminer une stratégie de communication à destination des clients partenaires et tiers pour préserver l'image de l'entreprise.»* **Non**, le but de résoudre le problème, pas de faire de la propagande.



Conclusion

1. Bien sûr, il faut tout faire pour ne pas être piraté,
2. Mais il ne faut pas se faire d'illusions, et prévoir le pire,
3. On peut survivre au piratage, mais moins à la perte de réputation. Ne faites donc pas comme la plupart des piratés.