ivanti

9 tendances de l'hameçonnage à connaître

Les attaques par hameçonnage existent depuis le milieu des années 90. Mais le passage mondial au télétravail (qui devient prioritaire) a accentué le problème, qui atteint désormais un niveau jamais vu depuis près de 30 ans.

Vous croyez que j'exagère ? Parlons-en :

80%

des professionnels de l'IT signalent une augmentation du nombre de tentatives d'hameçonnage l'an passé.

74%

des entreprises ont été les victimes d'une attaque par hameçonnage ces 12 derniers mois, dont 40 % au cours du dernier mois seulement.

Le département IT est désormais plus souvent ciblé que tous les autres groupes

- 21% Support client
- 35% Ventes
- **74% département IT**
- 27% personnel exécutif
- 25% Marketing

Le plus inquiétant ?

85% des professionnels de l'IT pensent que ces attaques sont plus sophistiquées que jamais.

Ce qui explique pourquoi

47% d'entre eux admettent s'être eux-mêmes laissés piéger.

+

48% des responsables de niveau C ont été des victimes.

Alors, que faire maintenant ?

96%

des entreprises forment leurs collaborateurs aux meilleures pratiques de cybersécurité. Et pourtant, malgré ces efforts, près de la moitié des professionnels de l'IT et des responsables de haut niveau ont été trompés par une attaque par hameçonnage.

Aujourd'hui, tout le monde, même les personnes les plus expérimentées et les plus au fait de la cybersécurité, peut être victime.

Alors peut-être est-il temps d'arrêter de croire que le problème vient de la formation et de comprendre que le coupable est simplement l'erreur humaine. Et il est sans doute temps d'éliminer l'erreur humaine de l'équation.

Le temps est peut-être venu du Zero Trust.

Découvrez comment le Zero Trust vous aide à stopper net les attaques par hameçonnage.

Commencez ici

The research in this infographic was conducted between April 30th - May 29, 2021 by MSI-ACI via an online questionnaire to 1,005 Business IT Professionals in the U.S., U.K., France, Germany, Australia and Japan.