



# PRINCIPALES CONCLUSIONS.

RAPPORT MONDIAL DE RENSEIGNEMENT  
SUR LES MENACES  
JUILLET – DÉCEMBRE 2024

Si l'activité des acteurs malveillants s'est intensifiée dans presque tous les domaines, certaines tendances se dégagent.

mimecast

RISK @ RADAR

01

## LES ACTEURS MALVEILLANTS EXPLOITENT LES SERVICES DE CONFIANCE

Les pirates informatiques tirent de plus en plus parti des plateformes de confiance telles que Microsoft, Google et Evernote pour héberger des contenus malveillants et lancer des attaques de phishing.

02

## LES MÉTHODES D'AUTHENTIFICATION COMPLEXIFIENT LES ATTAQUES MAIS L'IA FAVORISE LA CYBERCRIMINALITÉ

Les protocoles SPF, DKIM et DMARC donnent l'impression que les attaques proviennent d'une source fiable. Les attaques deviennent ainsi plus sophistiquées, tandis que la multiplication des chatbots basés sur l'IA permet aux cybercriminels d'acquérir toutes les compétences nécessaires en matière de piratage.

03

## LES TENSIONS GÉOPOLITIQUES ALIMENTENT LES CYBERATTAQUES

L'instabilité politique internationale, comme la guerre en Ukraine et les élections européennes, intensifie les cyberrisques, qui figurent, avec les menaces géopolitiques, en tête des préoccupations dans les dernières enquêtes.

04

## LE RISQUE D'ERREUR HUMAINE DEMEURE LE MAILLON FAIBLE

Les actions internes représentaient 68 % des failles de sécurité en 2023, tandis que 34 % des collaborateurs ont peur que leurs erreurs soient exploitées lors de futures attaques.

05

## L'USURPATION D'IDENTITÉ AINSI QUE LES LIENS ET FICHIERS MALVEILLANTS CONSTITUENT LES PRINCIPALES MENACES PAR UTILISATEUR

Les secteurs des arts, des spectacles et des loisirs, des services juridiques ainsi que des médias et de l'édition ont enregistré le plus grand nombre de menaces par utilisateur au second semestre 2024.

TÉLÉCHARGER LE RAPPORT