Piratage de cerveau : les innovations en matière d'ingénierie sociale en 2023

Ines Boutar

Regional field marketing manager

sosafe

28 Novembre 2023

INTERVENANT

Bref portrait

Ines Boutar

Regional Field marketing Manager

Contactez-moi !

sosafe

SOSAFE

Leader sur le marché de la sensibilisation et de la formation en Europe

Plus de 370 collaborateurs

Cybersécurité, psychopédagogie, développement de logiciels, design graphique, gamification

Plus de 3 000 clients

Avec des entreprises de toutes tailles et de tous secteurs, tels que la logistique, le secteur public, l'automobile, les infrastructures critiques, etc.

Plus de 2 300 000 utilisateurs

Plus de 60 modules d'apprentissage et vidéos
Plus de 600 modèles de phishing
Plus de 15 000 e-mails de simulation de phishing par jour

Ils nous font confiance

Marc O'Polo · SOS Children's Villages · CLARK · WWF · DeepL · ALDI · TSG · KP Snacks · CAP INGELEC · Groupe Le Duff · BUFAB

Pourquoi ils nous ont choisis...

Une approche scientifique

Micro-apprentissage narratif et gamifié pour un maximum d'engagement

Facile d'utilisation et évolutif

Une expérience fluide et personnalisée pour les administrateurs comme pour les utilisateurs

100 % conforme au RGPD

Approche de « privacy by design » avec des fonctions de signalement intelligent, conforme à ISO-27001

G2 Easiest To Do Business With Enterprise Summer 2023 · G2 Easiest To Use Enterprise Summer 2023 · G2 Leader Mid-Market Summer 2023 · G2 Users Love Us · G2 Leader Summer 2023 · 2023 Cybertech 100 · Cyber Security Excellence Awards Winner 2023 · Platin Security Awareness Security Insider Award 2022

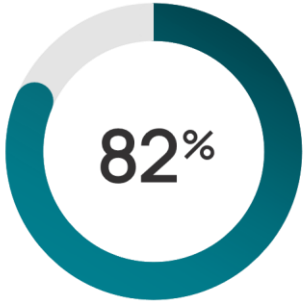

08:21
$00000000
100
grand theft auto
Vice city
Admiral

Les cybercriminels piratent nos cerveaux

Experts en psychologie humaine, ils savent manier cette arme avec dextérité

LE FACTEUR HUMAIN NE VARIE PAS

Les techniques d'ingénierie sociale restent le choix numéro 1 des cybercriminels



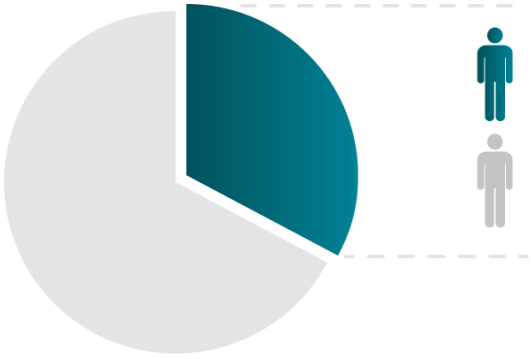
des violations de données impliquent le **facteur humain** (Verizon)

Top 3 des tactiques utilisées lors des cyberattaques réussies – toutes trois **impliquent le facteur humain**

1. Malware
2. Phishing
3. Ransomware

1 utilisateur sur **3**

clique sur les e-mails de phishing malveillants. Parmi eux...



1 utilisateur sur **2**

va jusqu'à divulguer des données sensibles.

sosafe

Source : Analyse du risque humain 2023, rapport « Data Breach Investigations Report » 2022 de Verizon

Analyse du risque humain 2023

- → **Vue d'ensemble** : rapport analytique sur l'état de la menace cyber en Europe avec ses récentes évolutions et ses stratégies
- → **Fondé sur les données** : enquête menée auprès de plus de **1 000** décideurs informatiques de toute l'Europe ; analyse réalisée à partir de plus de **8 millions de points de données** issus de la plateforme SoSafe
- → **Entretiens d'experts** : 9 interviews exclusives de RSSI actifs à l'international

Téléchargez-la ici !

Thomas Tschersich
RSI
Deutsche Telekom

Thomas Schumacher
Directeur général
Accenture Security

Jürgen Setzer
RSSI
Forces armées allemandes

Stéphane Duguin
PDG
CyberPeace Institute

Stefan Lüders
RSSI
CERN

Tobias Ludwichowski
RSSI
Signal Iduna

CYBERCRIMINALITÉ

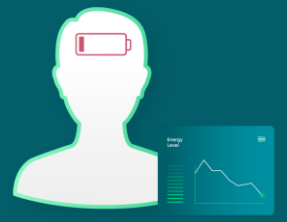
Nous sommes confrontés à des menaces cyber qui ne cessent de s'intensifier

1 Intelligence artificielle

2 Indétrônable phishing

3 Phishing multicanal

4 Pénurie de talents et burn-out



5 Attaques de la chaîne d'approvisionnement numérique

6 Rançongiciel

7 Crises géopolitiques

8 Échecs de la MFA

sosafe

Les événements mondiaux continuent de constituer des amorces parfaites pour les campagnes de phishing...

Géopolitique

Marianne

Israël-Iran : la cyber-guerre est déclarée

LA TRIBUNE

Guerre en Ukraine : les cyber-attaquants, l'autre armée de Vladimir Poutine

Le Point

Les Etats-Unis dénoncent une cyber-intrusion d'ampleur parrainée par la Chine

BFM TV

NANCY PELOSI À TAÏWAN: ENTRE PIRATAGE ET COUPURE, LA TENSION NUMÉRIQUE MONTE D'UN CRAN SUR L'ÎLE

Urgences sanitaires mondiales

Le Monde

Coronavirus : comment pirates informatiques et escrocs profitent de la pandémie

L'union

Si on vous propose par mail un «kit de protection» contre le Covid-19, attention à l'arnaque

Crises économiques et autres événements mondiaux

franceinfo:

Alertes arnaques : attention aux SMS qui proposent d'économiser sur la consommation énergétique

rfi

Séisme en Turquie et en Syrie: face à l'élan de solidarité, les escroqueries en ligne s'intensifient

sosafe

MANIPULATION ÉMOTIONNELLE

... et ces attaques atteignent leur but parce qu'elles font vibrer la corde sensible

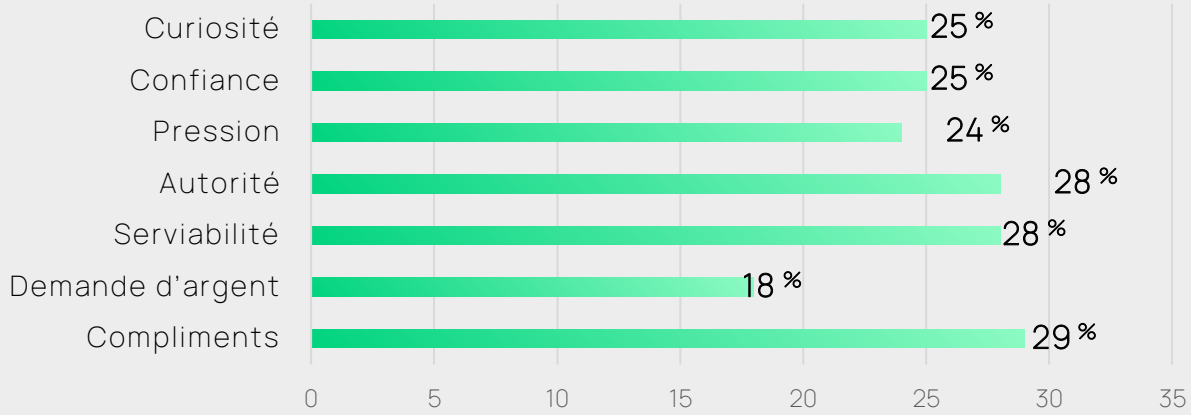
LADEPECHE.fr

Guerre en Ukraine : faux réfugiés, sites frauduleux... si vous souhaitez aider, gare aux arnaques !

« Chaque crise entraîne une **réponse émotionnelle** du grand public qui se mobilise pour donner à des œuvres humanitaires ou des associations caritatives. Il y a donc un afflux d'argent considérable qui attise la convoitise des criminels. C'est la raison pour laquelle ils ciblent tout particulièrement ce secteur, relativement démuni en matière de cybersécurité. »

Stéphane Duguin
PDG du CyberPeace Institute

Taux de clics par **facteur émotionnel déclenchant** en 2023



Top 5 des objets d'e-mails de phishing en 2022

1. **Véhicule accidenté** — Pression/Curiosité
2. **Invitation sur Teams** — Curiosité
3. **Erreur sur le salaire** — Pression/Curiosité
4. **Votre mot de passe Office expire aujourd'hui** — Pression
5. **Vous avez manqué une conversation sur Teams** — Pression/Curiosité

sosafe

Utilisée comme une arme, l'IA générative permet de créer des leurres de plus en plus efficaces

Exemple : le clonage vocal constitue un risque de plus en plus grand

Les attaquants réussissent à imiter artificiellement les voix de collègues ou de supérieurs hiérarchiques pour pousser les collaborateurs à :

→ Divulguer des informations sensibles

→ Déclencher des paiements depuis leur téléphone

74 % des professionnels de la cybersécurité pensent que l'intelligence artificielle va aggraver les menaces cyber

RTS Info

Deepfakes: le clonage vocal, la nouvelle menace pour l'identification en ligne

BDM

VALL-E : l'outil IA de Microsoft qui peut imiter la voix d'une personne

LES NUMERIQUES

35 millions de dollars volés grâce à une voix clonée par IA

Comment se protéger face à un secteur de cybercriminalité qui se professionnalise ?

APPROCHE HOLISTIQUE DU RISQUE HUMAIN

Nous devons adopter une approche plus holistique et développer une culture de la sécurité

Il faut promouvoir davantage de résilience et une solide culture de la sécurité au sein du capital humain

→ Intégration des sciences comportementales et des principes de la psychologie (p. ex., renforcement positif)

→ Formation continue

→ Portée étendue avec l'inclusion de nouvelles dimensions pour inciter à adopter des réflexes de sécurité

sosafe

Les experts en cybersécurité plébiscitent les méthodes de sensibilisation axées sur l'humain

1

Les formations personnalisées

qui adaptent l'expérience d'apprentissage en fonction des responsabilités des différents employés

2

La personnalisation des programmes

qui permet d'appliquer la charte graphique de la marque à la formation en ligne ou d'y intégrer les contenus et les polices de sécurité propre à l'entreprise

3

Des canaux conversationnels qui permettent des cycles plus rapides

alertent sur les nouvelles stratégies d'attaque ou dispensent des micro-apprentissages sur plusieurs points relatifs à la cybersécurité par le biais de différents outils de communication

Source : Analyse du risque humain 2023

Merci

Vous êtes intéressés ?
Contactez-moi

Ines Boutar
Regional field marketing manager

ines.boutar@sosafe.de

LinkedIn

sosafe