Julie Taton et Christophe Deborsu qui prêtent leur visage à la campagne contre l'hameçonnage. Ou pas ?

La campagne de Febelfin, 2ememain, le Centre pour la cybersécurité en Belgique, la Cyber Security Coalition, la police fédérale et le SPF Finances entend répondre au sentiment d'insécurité et à la multiplication des e-mails de phishing durant la crise du coronavirus.

EN BREF

- En ce moment, environ 20 % des e-mails de phishing sont liés à la crise du coronavirus.
- L'enquête d'Indiville menée à la demande de Febelfin montre que :
    - le sentiment d'insécurité en ligne s'accroît;
    - plus d'un Belge sur trois a reçu un message de phishing au cours du mois dernier. Chez les 35-49 ans, c'est même la moitié ;
    - un Belge sur quatre regrette les informations qu'il a transmises en ligne;
    - les 18-34 ans sont les moins prudents en ligne.
- Les entreprises ne sont pas épargnées. Les collaborateurs des services de gestion, des finances et des ventes sont ceux qui cliquent le plus souvent sur des e-mails de phishing.
- C'est une campagne de Febelfin en collaboration avec 2ememain, le Centre pour la cybersécurité en Belgique, la Cyber Security Coalition, la police fédérale et le SPF Finances. Au travers de cette nouvelle campagne sur le phishing, ces derniers souhaitent sensibiliser les consommateurs au fait qu'ils ne doivent jamais partager leurs codes bancaires personnels via un lien. Une banque ou toute autre entreprise fiable ne demandera jamais ce genre d'informations.
- 4 Belges célèbres « prêtent » leur visage à la campagne grâce à la deepfake technology (hypertrucage).
- Toutes les informations sur le phishing sont à retrouver sur la nouvelle plate-forme www.protegezvousenligne.be.

Avec la crise du coronavirus, les gens ont beaucoup de soucis en tête. 1,3 million de Belges vivent confinés à la maison dans un système de chômage temporaire. Pour beaucoup d'autres, le télétravail - combiné aux soins et à l'éducation des enfants - est devenu la nouvelle norme. Les gens s'inquiètent de la santé de leur famille et de leurs amis. A quoi s'ajoutent aussi d'éventuels problèmes financiers. Les fraudeurs profitent pleinement de cette distraction d'esprit. Recevoir un e-mail de phishing, le parcourir rapidement et cliquer sur le lien, c'est malheureusement devenu, aujourd'hui plus que jamais, un geste machinal.

Sans compter que les fraudeurs ne manquent pas de jouer sur l'actualité. Peut-on encore s'étonner que Google repère actuellement chaque jour dans le monde quelque 18 millions

d’e-mails de phishing ou contenant des logiciels malveillants concernant le coronavirus ? Autrement dit : environ 20 % de tous les e-mails de phishing font allusion au coronavirus.

Miguel De Bruycker, directeur du Centre pour la Cybersécurité Belgique : « Les cybercriminels jouent avec l'actualité. Ils savent quels thèmes nous intéressent. Par conséquent, soyez toujours sur vos gardes lorsque vous recevez des messages suspects contenant des liens sur un sujet d'actualité. »

Aujourd'hui, nous sommes tous plus numériques que jamais. Dans la mesure où de très nombreux magasins sont fermés, les gens commandent davantage en ligne. Pour les opérations bancaires aussi, il est conseillé d'opter pour le numérique. Or, les personnes qui franchissent aujourd'hui le pas vers la vie numérique qui est la nôtre en ce moment risquent d’être beaucoup plus réceptives au message de phishing des fraudeurs.

Enquête d’Indiville & Febelfin : le sentiment d'insécurité en ligne progresse

Une enquête effectuée par le bureau d'études Indiville à la demande de Febelfin (menée entre le 7 et le 10 avril auprès de 1.183 répondants, marge d'erreur de 2,3 %) montre que les Belges réalisent effectivement davantage d’opérations en ligne (64 % des répondants) et un groupe important déclare aussi effectuer des opérations bancaires numériques (+35 %) plus souvent qu'avant la crise du coronavirus.

Quatre Belges sur dix se sentent moins en sécurité en ligne depuis l'apparition du coronavirus.

39 % ont déclaré avoir reçu un message de phishing le mois dernier. Chez les 35-49 ans, on atteint même 48 %.

Les répondants ont largement conscience que les fraudeurs sillonnent le net pour essayer de les escroquer (97 % d’entre eux en sont conscients).

95% se disent prudents, car ils ne veulent pas devenir la proie des cybercriminels. 39 % des répondants font même des efforts supplémentaires pour sécuriser leurs opérations en ligne.

Ces chiffres sont-ils réalistes ? Le professeur Tim Smits, de l'Institut d'études des médias (Instituut voor Mediastudies - KU Leuven), nous donne son point de vue : « Une première remarque concernant les chiffres de cette enquête est qu'il s'agit ici exclusivement d'une question de perception. Ce que les gens pensent eux-mêmes de leur comportement ne correspond pas nécessairement à la réalité. Nous savons, grâce à la recherche, que les gens se sentent souvent plus intelligents que les autres. Le risque qu’ils soient en réalité moins prudents et moins attentifs au phishing est réel. À cet égard, il est frappant de constater qu'un Belge sur quatre a déjà transmis en ligne des données qu’il s’est senti par la suite mal à l'aise d’avoir communiquées. Cela donne matière à réflexion ».

L'enquête montre en effet que 23 % des Belges ont à un moment ou un autre transmis en ligne des informations qu’ils se sentent mal à l’aise d’avoir transmises. Ce chiffre est

alarmant, d'autant que nous constatons que ce groupe continue à courir un risque plus élevé de phishing et ne semble pas enclin à modifier son comportement :

- ce groupe affirme recevoir plus souvent des messages de phishing mais
- ce groupe répond aussi plus de deux fois plus souvent à un message de phishing (7 % au lieu de 3 %).

Enquête d'Indiville & Febelfin : les 18 à 34 ans, le groupe le plus imprudent

Ce qui est aussi frappant dans ces chiffres, c'est la relative négligence d'un certain nombre de jeunes de 18 à 34 ans. 9 % des personnes de cette catégorie d'âge reconnaissent ne pas être assez prudentes pour rester hors de portée des cybercriminels. C'est également la tranche d'âge qui a fait le moins d'efforts ces dernières semaines pour sécuriser ses opérations en ligne (27 % contre 39 % en moyenne).

Des fraudeurs toujours plus professionnels

Autre chose qui, bien sûr, ne facilite pas la vie des internautes : l'époque où les messages de phishing étaient truffés de fautes de français et se reconnaissaient donc en un clin d'œil est révolue. Tim Smits note ainsi aussi une professionnalisation croissante des messages de phishing. « Les cybercriminels diffusent des imitations convaincantes de communications commerciales bien réelles. Les sujets des messages visent la pertinence et suscitent la curiosité. Les fraudeurs se font passer pour des organismes officiels tels que des banques ou, au contraire, adoptent un ton très confidentiel comme on pourrait l'attendre de collègues ».

Ce dernier point n'est pas sans importance car de nombreux e-mails de phishing atterrissent dans les boîtes mail des collaborateurs. Chez Phished, une société spécialisée dans l'hameçonnage et l'ingénierie sociale, on en est bien conscient. Phished aide les entreprises en apprenant à leurs collaborateurs à reconnaître les attaques d'hameçonnage.

Selon Phished, les intitulés d'e-mails de phishing qui suscitent le plus de clics en cette période de crise du coronavirus sont :

- IT : comment se connecter avec le siège.
- Microsoft : X a partagé un fichier avec vous.
- Office 365 : Your administrator has updated your account.
- Votre commande a été envoyée !

Pendant la pandémie actuelle, certains départements d'entreprise semblent courir plus de risques de tomber dans le piège du phishing que d'habitude, explique Arnout Van de Meulebroucke, COO de Phished. « Alors qu'en temps normal, ce sont les collaborateurs des services généraux qui sont les plus susceptibles de répondre aux messages de phishing (22,9 %), suivis par les services de vente (20,81 %) et les finances (19,4 %), les trois services qui cliquent aujourd'hui le plus sur ces messages sont le département des finances (29,43 %), suivi du service des ventes (27,03 %), le département management (24,59 %) clôturant ce trio de tête. »

Comment reconnaître le phishing ?

Nous l’avons dit, vous ne reconnaîtrez donc pas un message de phishing aux fautes de français ni à son objet, qui est souvent crédible. Alors, comment reconnaître le phishing ?

Eh bien, tous les messages de phishing ont une chose en commun : ils demandent vos codes bancaires personnels (souvent vos codes pour la banque en ligne) via un lien.

Donc, si vous recevez un tel message, une alarme doit immédiatement résonner dans votre esprit : le message est un faux ! Votre banque ne vous demandera jamais vos codes via un lien. Pas pour une mise à jour de sécurité, pas pour renouveler ou (dé)bloquer votre carte bancaire, ... D'autres entreprises et organisations fiables ne le feront jamais non plus.

C'est également la clé de voûte de la dernière campagne contre le phishing de Febelfin, qui sera lancée aujourd'hui.

« Des tentatives de phishing, il y en a toute l'année et il est typique que les fraudeurs s'adaptent constamment aux circonstances », explique Karel Baert, CEO de Febelfin.
« Nous constatons également que les e-mails, les SMS et autres messages ont une apparence de plus en plus professionnelle et qu'il devient toujours plus difficile de distinguer le vrai du faux. C'est pourquoi nous ne nous concentrerons pas dans cette campagne sur la manière de détecter les faux messages. Notre message est plutôt : soyez attentifs à tout ce qui sort de l’ordinaire. Votre banque ne vous demandera jamais de transmettre vos codes personnels. Alors ne le faites jamais ».

Notre nouvelle campagne de sensibilisation contre le phishing utilise le deepfake

4 Belges célèbres ont « prêté » leur visage à notre campagne contre le phishing. Du côté francophone, il s’agit de Julie Taton et de Christophe Deborsu. Du côté néerlandophone, on retrouve Leah Thijs (Marianne van Thuis) et Thomas Vanderveken.

Et le terme « prêter » est on ne peut plus adéquat ici car aucun des quatre ne s’est jamais trouvé sur notre plateau de tournage. Febelfin a en effet fait appel à la deepfake technology (hypertrucage) qui permet de recomposer des images humaines via une intelligence artificielle. Autrement dit : nous avons collé la tête de nos quatre principaux acteurs sur le corps d'un inconnu. Le résultat est donc totalement faux, tout comme la demande d'une banque de partager vos codes via un lien.

La campagne, passant par des vidéos et des bannières, sera diffusée sur tous les supports numériques du secteur financier (de Febelfin et des banques) : sites internet, applications mobiles, distributeurs automatiques, écrans numériques dans les agences, canaux de médias sociaux, newsletters, ...

À partir d'aujourd'hui, 4 mai, la campagne sera également diffusée sous la forme d’un message d'intérêt public sur les chaînes de télévision de RTL et de la VRT.

Christophe Deborsu : « Le film est si bien fait que la possibilité de doute existe encore. Et c'est exactement le message de mise en garde de cette campagne : en ligne vous pouvez

faire passer des choses fausses comme réelles. Si vous soupçonnez que quelque chose cloche, ne vous en approchez pas. Je ne me fais pas d'illusion: même en ces temps difficiles, les criminels trouvent toujours de nouveaux moyens de nous voler. Comme vous, je rêve d'un monde meilleur. Mais en attendant: réagissons !»

Julie Taton : « Bien sûr, je sais que ce n'est pas moi dans la vidéo de Febelfin, mais je peux tout à fait m'imaginer que des gens se fassent piéger. C'est un double sentiment : en temps de corona, on nous rappelle à quel point la technologie est fantastique. Nos applications nous permettent d'effectuer toutes les transactions bancaires et d'acheter en ligne. C'est un grand luxe. En même temps, il faut toujours rester très vigilant et continuer à faire la distinction entre ce qui est plausible et ce qui ne l'est pas. Une chose est sûre : ma banque ne me demandera jamais mes codes par téléphone, par email ou par SMS. »

La campagne bénéficie du soutien de nombreuses entreprises et des pouvoirs publics, notamment par l'intermédiaire du Centre pour la cybersécurité en Belgique, de la Cyber Security Coalition, de la police fédérale et du SPF Finances. Tous ces partenaires contribueront à diffuser la campagne via leurs canaux respectifs.

2ememain est partenaire de notre campagne et sensibilisera les acheteurs en diffusant son propre message

Aleksandra Vidanovski, porte-parole de 2ememain : « Les cybercriminels sont ingénieux et créatifs. C'est pourquoi, lorsque la crise du coronavirus a éclaté, nous étions tout de suite à l'oeuvre pour faire disparaître de notre plate-forme toutes les publicités pour les masques buccaux et les gels désinfectants. Non seulement parce que nous désapprouvons le fait que, dans de nombreux cas, des prix exorbitants étaient facturés pour ces produits rares, mais aussi parce que nous savons que ce sont précisément ces produits qui sont utilisés de manière abusive pour des publicités frauduleuses ou fictives ».

2ememain continue par ailleurs à travailler sur des outils visant à encore mieux sécuriser la plate-forme et à se débarrasser des fraudeurs.

« Cependant, l'information et la sensibilisation de nos visiteurs demeure l'outil le plus important. Nous vous invitons ainsi à faire preuve à tout moment de prudence et de vigilance. La façon d'opérer des fraudeurs est en fait souvent la même : ils essaient de vous détourner de notre plate-forme et vous demandent d'introduire vos coordonnées bancaires sur un faux site de paiement ou un faux site d'une société de livraison qui semble souvent fiable. Une fois que vous êtes "connecté/e", les escrocs peuvent mettre la main sur tout ce qui vous appartient. C'est pourquoi nous vous recommandons de ne jamais effectuer un paiement par l'intermédiaire d'un site que vous n'utilisez pas habituellement. Nous travaillons également d'arrache-pied pour pouvoir bientôt proposer des outils qui permettront aux utilisateurs de rester sur notre plate-forme tout au long du processus de vente ou d'achat », conclut Aleksandra Vidanovski.

2ememain a rassemblé tous les conseils pour permettre aux utilisateurs d'agir en toute sécurité sur cette page : https://www.2ememain.be/i/securite/.

Une victime d'hameçonnage raconte son expérience : « On m'a vidé mon compte »

À 45 ans, Inge a récemment été victime d'un hameçonnage. Elle se rappelle encore dans les moindres détails comment s'est déroulée l'escroquerie. « Cela s'est passé au début du confinement, le dimanche 22 mars vers midi. J'étais occupée à faire plusieurs choses : préparer à manger, dresser la table, je devais aider mon fils, etc. Juste à ce moment-là, j'ai reçu un SMS d'un numéro de téléphone inconnu. Le message indiquait que ma carte bancaire venait d'être utilisée pour se connecter à l'application de ma banque. S'il ne s'agissait pas de moi, je devais vérifier la connexion frauduleuse via un lien qui se trouvait dans le SMS. Ce n'est qu'après coup que je me suis rendu compte que toutes sortes de choses ne concordaient pas : j'avais ma carte à portée de main, ma banque ne me prévenait jamais de la sorte et le nom de domaine du lien était suspect. Mais sur le moment même, j'ai cliqué sur le lien et je suis tombée sur une reconstitution du site de ma banque où je me suis connectée avec mon lecteur de carte. Un message d'erreur s'est alors affiché, j'ai reçu un nouveau SMS et j'ai une nouvelle fois tenté de me connecter. »

Inge s'est alors replongée dans la préparation de son repas, puis a consulté le solde de son compte sur l'application de sa banque. « J'étais anéantie. J'ai vu deux transactions de 2 000 euros par virement et encore un de 500 euros. Après un dernier virement de 9 euros, mon compte était totalement vide. »

Inge a porté plainte à la police, bloqué sa carte de banque et ouvert un dossier pour fraude auprès de sa banque. « La police m'a fait savoir plus tard que l'argent viré avait été immédiatement retiré par ce qu'elle appelle une mule. Ce que je possédais est donc parti je ne sais où. Je suis une mère célibataire, avec des revenus limités et le coût de la vie est élevé. La banque m'a entre-temps informée que je serai indemnisée. J'estime qu'il est essentiel d'attirer l'attention sur ce genre de fraude, car une amie a reçu le même SMS il y a quelques jours. Les criminels derrière cette escroquerie continuent donc leur petit numéro. »

Toutes les informations sur le phishing en un coup d'œil

Dans le cadre de sa campagne, Febelfin renvoie toujours vers la plate-forme en ligne www.protegezvousenligne.be. Les visiteurs peuvent y retrouver toutes les informations pratiques sur l'hameçonnage. De quoi s'agit-il ? À quoi devez-vous faire attention ? Que devez-vous faire ou ne pas faire ? Et où vous adresser si vous êtes tombé/e dans le piège ? Le site sera mis en ligne le 4/5. Pour en avoir un aperçu, vous pouvez vous logger à l'aide de ces identifiants : ldv / ldvunited

Et quid des autres formes de fraude ?

Bien entendu, les fraudeurs n'envoient pas que des courriels de phishing renvoyant au coronavirus. Ils essaient d'escroquer les gens de toutes les manières possibles : en bloquant leur ordinateur et en réclamant une rançon, ou simplement en leur vendant des choses qui n'existent pas.

Le Commissaire Olivier Bogaert de la Police fédérale : « Les cybercriminels s'empressent de jouer sur les inquiétudes de la population concernant le coronavirus. Ils peuvent ainsi envoyer de faux messages indiquant que le virus a été détecté chez un membre de la

famille de leur victime. L'idée est que le destinataire clique impulsivement sur un lien qui installera un programme sur son ordinateur ou son smartphone et rendra l'appareil inutilisable, à moins de payer une rançon. Il s'agit d'une variante du classique rançongiciel que les criminels utilisent pour verrouiller l'ordinateur ou le smartphone de leur victime. Notre conseil standard pour ce type de message est le suivant : gardez la tête froide, ne réagissez pas immédiatement mais vérifiez la source du message. Par exemple, recherchez l'origine du message dans le moteur de recherche de Google. Comme il s'agit de tentatives de fraude opérées à un niveau international, il y a de fortes chances que Google puisse déjà vous mettre en garde. Nous voyons également des messages frauduleux circuler par e-mails, SMS et sur les médias sociaux concernant de faux médicaments, des masques buccaux, des gants... Et même des cadeaux pour les hôpitaux. Si vous répondez à ces offres ou sollicitations, vous allez vous retrouver escroqué/e et aurez partagé vos informations privées avec des fraudeurs. Notre conseil : ne cliquez pas sur les messages suspects, achetez uniquement sur des boutiques en ligne de confiance et vérifiez que l'identité de l'expéditeur d'un message est authentique avant de répondre à celui-ci".

Annexes

Banners

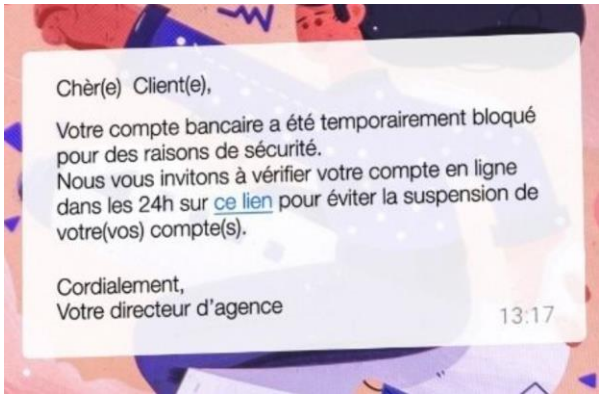
Vous pouvez télécharger les banners via ce lien : https://we.tl/t-6f4OQ4ZYxq

Vidéos

Vous pouvez télécharger les vidéos :

Christophe: https://youtu.be/dh0J2JxMHwg
Julie: https://youtu.be/mY6-bzb9Tao

Exemples de message de phishing liés au coronavirus



Bonjour JP

Si vous ne l'avez pas déjà entendu, Bitcoin devrait atteindre $100.000 avant la fin de l'année! 5 fois plus élevé que son sommet de 2017.
Les projections viennent après que de grandes entreprises, dont Facebook et Uber, ont annoncé qu'elles entreraient dans l'arène de la cryptographie cette année.
Nous vous offrons une place dans notre plateforme d'investissement privé - Vous pouvez enregistrer votre compte gratuit tout de suite et commencer votre voyage dès aujourd'hui.
Votre coût d'investissement: $250
Créer un compte gratuit

Meilleures salutations,
BTC-Era

Unsubscribe

Résultats complets de l'étude de Phished

Q: Type de sujet (quels *Objets de message* sont populaires ?)
A: En période normale, le top 10 se compose des « *Objets de message* » suivants :

- SharePoint: Your files are being deleted soon.
- Microsoft: {{ SpearPhishingFirstName }} {{ SpearPhishingLastName }} a partagé un fichier avec vous.
- Office 365: Your administrator has expired your password.
- Votre colis est en route !
- Réinitialisez votre mot de passe (pour info : LinkedIn)
- LinkedIn: {{ SpearPhishingFirstName }} has invited you
- Un nouveau document est disponible pour vous (pour info: de myworkandme)
- AMENDE [#644733573] – Procès-verbal
- Pourquoi as-tu mis ça online ??
- Pouvez-vous approuver ce devis?

Q: Pendant la crise du coronavirus, les *Objets de message* suivants sont devenus des incontournables :

- IT: Comment se connecter au siège social.
- Microsoft: {{ SpearPhishingFirstName }} {{ SpearPhishingLastName }} a partagé un fichier avec vous.
- Office 365: Your administrator has updated your account.
- Votre colis est en route !
- Votre colis est en retard!
- LinkedIn: {{ SpearPhishingFirstName }} has invited you
- Un nouveau document est disponible pour vous (pour info: de myworkandme)

- AMENDE [#644733573] – Procès-verbal
- Mesures contre le coronavirus: Mise à jour
- Vous pouvez m’expliquer ceci?

Q: À quel moment de la journée et quel jour clique-t-on le plus ?
A: En termes de chiffres absolus, le lundi est le jour de phishing par excellence. Ce sont surtout les mails de spear-phishing qui fonctionnent bien : des mails ciblés de la part de (soi-disant) patrons ou collègues.

Le taux moyen de phishing est également plus élevé le mardi. Dans ce cas-ci, les mails frauduleux qui fonctionnent le mieux sont ceux qui concernent toutes sortes de transactions (comme : ‘nous avons bien reçu votre commande’ ou ‘votre paiement est validé’). C'est pourquoi les courriers de services postaux tels que PostNL ou bpost fonctionnent bien aussi.

Q: Les employés de BE sont-ils plus réceptifs d’être victimes de phishing que leurs collègues des pays cités dans l'article ?
A:
Les employés belges sont en effet légèrement plus sensibles aux tentatives de phishing que les employés d'autres pays.
En Belgique, la prise de conscience du problème est moins répandue que dans ces autres pays, c’est là que se situe la différence.

Q: Quels départements de l’entreprise sont les plus vulnérables ?
Période normale:

1. Office – 22.90%
2. Sales – 20.81%
3. Finance – 19.40%
4. Management – 19.32%
5. Marketing – 16.57%

Crise du coronavirus:

1. Finance – 29.43%
2. Sales – 27.03%
3. Management – 24.59%
4. HR – 22.56%
5. Operations – 17.86%

Il est frappant de constater que ce sont précisément les employés du département financier qui mordent davantage à l’hameçon pendant cette crise.

Q: La crise du coronavirus a-t-elle un impact?
A: De manière générale, le pourcentage moyen de phishing se maintient autour des 20 %, tant en période normale que pendant la crise du coronavirus. Le taux moyen de clics reste donc à peu près le même. Cependant, nous constatons un changement évident dans la façon dont les départements cliquent sur les simulations.
Nous constatons bien une augmentation du nombre de tentatives de phishing, de sorte que l’on peut effectivement dire que le risque d'une attaque de phishing destructive est nettement plus élevé.
Pour résumer : en moyenne, il n’y a pas plus d’employés qui mordent à l’hameçon qu’en temps normal, mais à l’échelle mondiale, le nombre de tentatives de phishing monte en flèche: donc oui, la crise du coronavirus a un impact.