proofpoint.

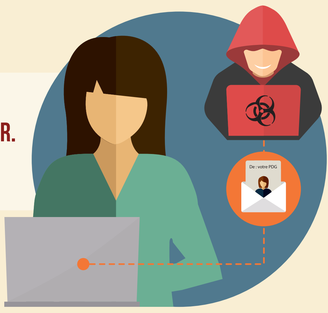
LE FACTEUR HUMAIN 2017

Les e-mails malveillants exploitent la nature humaine, pas le code informatique.

Voici les principales techniques utilisées par les cybercriminels en 2016 pour inciter les utilisateurs à interagir avec les messages électroniques malveillants et les publications sur réseaux sociaux.

LE PIRATAGE DE LA MESSAGERIE EN ENTREPRISE (BEC) EST EN PLEIN ESSOR.

Le volume de messages d'attaques BEC est passé de 1% en 2015 à **42% fin 2016**.



LE PHISHING VIA DES COMPTES DE RÉSEAUX SOCIAUX S'INTENSIFIE.

Ce type de phishing a connu une **hausse de 150%** en 2016.

LA DISTRIBUTION DES MALWARES VARIE SELON LEUR CATÉGORIE ET LE JOUR DE LA SEMAINE.

Les campagnes de diffusion de ransomwares sont **déployées de préférence du mardi au jeudi**.

LE TEMPS, C'EST DE L'ARGENT.

87% des clics sur des URL malveillantes sont effectués dans les 24 heures qui suivent la remise de l'e-mail.

Près de 50% des clics se produisent dans l'heure.

25% des clics interviennent en à peine 10 minutes.

LES ATTAQUES CULMINENT EN MILIEU DE JOURNÉE.

L'activité de clics atteint son maximum 4 à 5 heures après le début de la journée ouvrable, soit vers l'heure du déjeuner.

LES UTILISATEURS SE LAISSENT BERNER PAR LES APPLICATIONS MOBILES FRAUDULEUSES.

Les applications malveillantes **utilisent des noms trompeurs et des éléments distinctifs des marques usurpées** pour convaincre les utilisateurs de télécharger des malware.

PLUS DE TÉLÉPHONES MOBILES ET DONC PLUS DE RISQUES...

42% des clics sur les URL malveillantes émanent d'appareils mobiles, soit **plus du double du taux de l'an dernier, qui était de 20%**.

TÉLÉCHARGEZ LE RAPPORT COMPLET

proofpoint.com/fr/human-factor-report-2017