

Qu'est-ce que le Doxing ?



Muriel de MARCOS
Présidente Directrice Générale
M.G.M Solutions

Le Doxing, également écrit Doxxing, fait référence à la divulgation en ligne des informations personnelles d'une personne. Cette pratique constitue une forme de harcèlement en ligne où l'on expose publiquement le vrai nom, l'adresse, l'emploi ou d'autres données d'identification d'un individu, sans son consentement, dans le but de l'humilier ou de le harceler. Le terme "Doxing" est dérivé du mot "documents".

Dans la culture des pirates informatiques des années 1990, le terme a été abrégé en "docs", puis en "dox", désignant la récupération de documents ou d'informations personnelles, telle que l'adresse physique d'une personne, pour ensuite les publier sur Internet. C'est grâce au collectif de hackers Anonymous que le terme s'est popularisé auprès du grand public.

Le Doxing de nos jours se réfère à la divulgation en ligne des informations personnelles d'une personne sans son consentement. Il peut également être utilisé pour dévoiler l'identité réelle derrière un

pseudonyme anonyme et la rendre publique.

Certaines attaques de Doxing sont motivées par le harcèlement ou la vengeance, tandis que d'autres ciblent des individus qui publient anonymement des commentaires racistes ou propagent un discours haineux en ligne.

Bien que cette pratique existe depuis plusieurs décennies, elle est toujours présente et représente un risque significatif. Une fois que des informations telles que l'adresse physique, le lieu de travail, le numéro de téléphone, ou l'adresse e-mail d'une personne sont divulguées, celle-ci devient vulnérable et susceptible d'être ciblée.

Les attaques de Doxing peuvent aller des plus innocentes, telles que de fausses inscriptions à des listes de diffusion ou des livraisons de pizzas, aux plus dangereuses, comme le harcèlement des proches ou de l'employeur de la victime, le harcèlement physique, le swatting, l'usurpation d'identité, les menaces et autres formes de cyberharcèlement.

La pratique du Doxing demeure répandue et présente des dangers réels pour la sécurité en ligne et la protection des informations personnelles des individus.

Certains individus pratiquant le Doxing se procurent des informations personnelles sur leurs cibles en faisant appel à des courtiers en données. Ces entreprises, qui vendent généralement ces données aux annonceurs, proposent également des moteurs de recherche de personnes offrant des dossiers complets à quiconque en fait la demande.

Les courtiers en données collectent ces informations via divers canaux, tels que les documents publics

(actes de mariage, permis de conduire, registres électoraux), les cartes de fidélité (pour connaître les habitudes d'achat en ligne et hors ligne), l'historique des recherches (recherches effectuées, sites visités, téléchargements), et même en achetant des informations à d'autres courtiers en données. Cette pratique soulève des préoccupations concernant la confidentialité et la sécurité des informations personnelles en ligne.

Impacts du Doxing : des cas concrets

Le Doxing peut toucher n'importe qui, car il suffit qu'une personne ne vous apprécie pas ou soit en désaccord avec vous pour prendre la peine de compiler et de divulguer vos informations personnelles.

Parmi les victimes du Doxing, on retrouve notamment :

Médecins pratiquant des IVG : certains professionnels de la santé, tels que des médecins réalisant des interruptions volontaires de grossesse (IVG), ont été ciblés par des individus hostiles cherchant à exposer leur identité, leur adresse et d'autres informations dans le but de les intimider ou de les harceler.

Personnes innocentes accusées à tort de crimes : il arrive que des individus innocents soient faussement accusés de crimes ou de délits. Dans certains cas, des personnes mal intentionnées ont publié leurs informations personnelles en ligne, les exposant ainsi à des conséquences préjudiciables et injustifiées.

Membres de groupes racistes : les personnes affiliées à des groupes racistes ou extrémistes peuvent également être la cible de Doxing. Leurs informations personnelles peuvent être divulguées dans le but de les dénoncer publiquement ou de les exposer à des représailles.

Représentants des forces de l'ordre : les membres des forces de l'ordre, tels que les policiers, peuvent être visés par des individus cherchant à les identifier et à révéler leurs informations personnelles en ligne, souvent à la suite d'incidents controversés ou des événements médiatisés.

Le Doxing peut avoir de graves répercussions sur la vie des personnes touchées, causant des dommages émotionnels, sociaux et professionnels. Il met en lumière l'importance de protéger la vie privée en ligne et de prendre des mesures pour se prémunir contre de telles attaques malveillantes.

Que faire en cas de Doxing ?

Si vous avez été victime de Doxing ou si vous soupçonnez d'être exposé à cette pratique, il est crucial d'agir rapidement pour limiter les dommages potentiels.

Voici quelques mesures simples à prendre immédiatement en cas de Doxing :

Collectez des preuves

Prenez des captures d'écran de toutes les informations exposées en ligne. Ces preuves peuvent être utiles pour des actions ultérieures, y compris en cas de signalement aux autorités.

Signalez le Doxing aux plates-formes concernées

Si vos informations personnelles ont été divulguées sur des réseaux sociaux, sites web ou forums, signalez ces contenus aux administrateurs des plates-formes. De nombreuses plates-formes ont des politiques strictes contre le Doxing et prendront des mesures pour supprimer ces informations.

Signalez le crime aux autorités compétentes

Le Doxing est souvent considéré comme un cybercrime. N'hésitez pas à signaler cette infraction aux autorités locales compétentes, qui pourront enquêter sur l'affaire.

Renforcez la sécurité de vos comptes

Changez vos mots de passe pour des combinaisons solides et utilisez un gestionnaire de mots de passe sécurisé pour les stocker. Activez l'authentification à deux facteurs pour une couche de sécurité supplémentaire. Vérifiez et renforcez également les paramètres de confidentialité de vos comptes en ligne.

Cherchez du soutien auprès de vos proches

Le Doxing peut être éprouvant émotionnellement. N'hésitez pas à parler de la situation à vos amis et à votre famille pour obtenir du soutien et du réconfort.

Envisagez de changer de coordonnées

Si les informations divulguées sont particulièrement sensibles, envisagez de changer votre numéro de téléphone, votre nom d'utilisateur ou d'autres éléments d'identification afin de préserver votre vie privée et votre sécurité.

En prenant rapidement ces mesures, vous pourrez mieux protéger vos informations personnelles et atténuer les conséquences potentielles du Doxing.

Comment vous prémunir du Doxing ?

Limitez les informations personnelles en ligne

Ne partagez pas d'informations sensibles comme votre adresse, numéro de téléphone, adresse électronique principale ou détails financiers sur les réseaux sociaux ou autres plateformes publiques.

Utilisez des pseudonymes

Si possible, utilisez des pseudonymes pour vos comptes en ligne, surtout sur des forums ou sites où vous ne connaissez pas les autres utilisateurs.

Renforcez vos paramètres de confidentialité

Réglez vos paramètres de confidentialité sur les réseaux sociaux pour que seules les personnes de confiance puissent voir vos informations

personnelles. Vérifiez et mettez à jour ces paramètres régulièrement.

Surveillez les informations publiques vous concernant

Effectuez régulièrement des recherches sur votre nom pour voir quelles informations sont accessibles publiquement. Si vous trouvez des informations sensibles, contactez le site pour les faire supprimer.

Utilisez des e-mails et numéros de téléphone temporaires

Pour les inscriptions sur des sites moins sûrs, utilisez des e-mails et numéros de téléphone temporaires.

Évitez de partager des documents sensibles

Ne partagez pas de documents personnels comme votre carte d'identité, passeport ou factures en ligne, sauf si absolument nécessaire et uniquement sur des sites sécurisés.

Sensibilisez votre entourage

Parlez à vos amis et à votre famille de l'importance de ne pas partager vos informations personnelles sans votre consentement.

En suivant ces quelques conseils, vous pouvez réduire considérablement le risque de Doxing et protéger votre vie privée en ligne.

L'information et la transmission sont des actions fondamentales afin d'anticiper des risques majeurs pouvant être à terme, destructeurs.

Grâce aux actions combinées de tous, nous pouvons créer un environnement numérique plus sûr.