L'usurpation d'identité sur Internet

eHealth actuel

Reinhold Sojer

Dr, collaborateur scientifique eHealth, FMH

En cas de «vol» d'identité, les données personnelles sont utilisées de façon abusive par des criminels, soit à des fins d'enrichissement, soit pour porter préjudice à la victime. Comme l'identité n'est pas quelque chose qui, en soi, peut être volée, on parle plus communément d'usurpation d'identité. Il est prévu d'inscrire ce terme dans le droit pénal suisse dans le cadre de la révision totale de la Loi fédérale sur la protection des données et de la modification d'autres textes relatifs à la protection des données.

L'usurpation d'identité est toujours réalisée en deux étapes:

1. d'abord par le vol de données personnelles,
2. ensuite, les données volées sont utilisées pour commettre un abus ou une escroquerie.

Pour une usurpation d'identité, quelques données telles que le nom, l'adresse ou la date de naissance suffisent.

Pour accéder aux données personnelles qui servent à identifier un individu dans le monde numérique, le cybercriminel procédera par espionnage ou au moyen d'une attaque sur des données d'utilisateur volées chez des prestataires de services en ligne. Pour une usurpation d'identité, quelques données telles que le nom, l'adresse ou la date de naissance suffisent. Ces données personnelles sont souvent demandées lors de l'inscription auprès de services en ligne, notamment sur les réseaux sociaux, ou pour l'identification de l'appelant lors de contrats téléphoniques.

Le cas du groupe Internet Yahoo montre l'ampleur qu'une attaque peut prendre: en août 2013, Yahoo avait annoncé être victime d'une cyberattaque. En 2017, on a appris que les données personnelles de plus de 3 milliards de comptes avaient été volées lors de cette attaque. Les cybercriminels avaient obtenu l'accès à des données telles que les noms, adresses e-mail ou numéros de téléphone, des données intéressantes pour d'autres attaques et susceptibles d'être utilisées de façon ciblée pour une usurpation d'identité.

Ces données volées permettent d'effectuer des commandes de marchandises au nom de la victime et de diffuser de fausses informations visant à nuire à la réputation de certaines personnes ou à les intimider. D'après le *Breach Level Index* (breachlevelindex.com), une base de données mondiale pour l'enregistrement des violations de la sécurité et de la protection des données, l'augmentation du vol de données de santé est particulièrement frappante. En 2015, le deuxième assureur-maladie aux Etats-Unis, Anthem, a été victime d'une cyberattaque lors de laquelle les données de 78 millions d'assurés ont été volées. Même si aucune donnée médicale n'a été directement affectée, l'escroquerie à l'assurance ou le chantage à l'aide de données personnelles représentent un potentiel de dommage important. Mais le summum est atteint lorsque les cybercriminels parviennent à obtenir les mots de passe.

Phishing = Password + Harvesting + Fishing

Les méthodes de l'ingénierie sociale (social engineering), qui visent à abuser de la serviabilité, de la bonne foi ou de l'insécurité des personnes, sont utilisées pour accéder à des données confidentielles. Une méthode très répandue pour espionner des mots de passe est le *phishing*. Le mot phishing se compose des mots anglais «password», «harvesting» et «fishing». Il permet d'induire en erreur l'utilisateur par des e-mails, sites web ou messages Twitter falsifiés pour obtenir des données d'accès personnelles. Généralement, l'expéditeur est une organisation connue ou, lors d'une escroquerie financière, il s'agit d'une banque. Des maliciels peuvent également être utilisés pour conduire une personne sur un site web malveillant (par ex. pirate de navigateur). Si l'hameçonneur vise les données d'accès pour des services en ligne, il envoie un courriel indésirable

Les applications telles que Twitter, WhatsApp, Facebook, Instagram ou Google Translate rassemblent sans cesse des données personnelles.

Published under the copyright license "Attribution – Non-Commercial – NoDerivatives 4.0". No commercial reuse without permission. See: http://emh.ch/en/services/permissions.html

(spam) de manière aléatoire au plus grand nombre possible de personnes en espérant que des clients du service en ligne qu'il a pris pour cible figureront parmi les destinataires et qu'ils réagiront. Une méthode plus efficace consiste à envoyer des e-mails frauduleux en utilisant des adresses achetées ou hackées, comme dans le cas de Yahoo. Dans une prochaine étape, le destinataire est prié, sur le faux site web, de s'identifier avec son nom d'utilisateur et son mot de passe, et le tour est joué, les cybercriminels ont obtenu les données qu'ils voulaient. Depuis un certain nombre d'années, les attaques d'hameçonnage sont aussi combinées avec les rançongiciels, des logiciels malveillants (voir BMS 2016;97(49–50):1708–9).

Une forme particulière d'hameçonnage est le «Spear-Phishing», où le cybercriminel connaît non seulement l'adresse e-mail de la victime, mais aussi des détails sur sa vie privée et professionnelle. Le cybercriminel peut se servir du nom d'une personne ou organisation de confiance pour conduire, par exemple par e-mail ou par Facebook, la victime à exécuter certaines actions spécifiques. C'est selon cette procédure qu'en été 2016, en Allemagne, des messages avec l'expéditeur hq.nato.int contenant des informations sur le putsch militaire en Turquie et un lien vers un site web compromis par des codes malveillants ont été envoyés à des politiciens allemands.

Plus les données espionnées auprès de la victime sont personnelles, plus le message frauduleux semblera authentique. Les applications telles que Twitter, WhatsApp, Facebook, Instagram ou Google Translate rassemblent sans cesse des données personnelles, ont accès à des données de contact, de calendriers ou de localisation, et savent qui vous êtes.

Correspondance:
Dr rer. biol. hum.
Reinhold Sojer
Wissenschaftlicher Mitarbeiter / Stv. Leiter Abteilung Digitalisierung / eHealth
FMH Verbindung der Schweizer Ärztinnen und Ärzte
Elfenstrasse 18
Case postale 300
3000 Berne 15
Tél. 031 359 12 04
reinhold.sojer[at]fmh.ch

Comment peut-on se protéger ?

Il n'est pas possible de se protéger à 100% contre l'usurpation d'identité. D'une part, parce que les données personnelles sont sauvegardées dans diverses institutions (banques, assurances, hôpitaux, etc.) et qu'il est difficile de les influencer. D'autre part, les cybercriminels opèrent généralement de façon professionnelle pour usurper des identités. Les méthodes présentées dans cet article ne représentent qu'une petite partie de celles qui sont utilisées aujourd'hui. De plus, elles sont souvent associées à des méthodes en dehors du monde numérique, par ex. le *Dumpster Diving* (la fouille des déchets à la recherche de données personnelles).

- Familiarisez-vous avec le thème de l'usurpation d'identité, car un homme averti en vaut deux.
- Protégez-vous de maliciels en maintenant vos systèmes à jour et en installant systématiquement les mises à jour de sécurité (pour les recommandations, voir BMS 2016;97(49–50):1708–9).
- Ne saisissez les données personnelles qu'avec retenue et uniquement sur des sites web et portails dignes de confiance. N'utilisez jamais votre vraie date de naissance sur les réseaux sociaux.
- Méfiez-vous des e-mails que vous recevez spontanément et soyez prudent si vous recevez des e-mails qui vous demandent une action et vous menacent de conséquences en cas de non-exécution.
- Les réseaux Wi-Fi publics comportent le risque d'être écoutés par des tiers. Si vous échangez des informations sensibles, vous devez les protéger par un cryptage supplémentaire (HTTPS, VPN ou plugiciels spéciaux).

Il n'est pas possible de se protéger à 100% contre l'usurpation d'identité.

- N'utilisez jamais les mêmes mots de passe pour différents comptes Internet et modifiez-les de temps à autre. L'utilisation de noms d'utilisateur différents pour des services en ligne complique la tâche des hameçonneurs pour établir un profil complet de votre identité.
- Utilisez si possible toujours l'authentification à deux facteurs (2FA). Cette vérification en deux étapes exige, outre un nom d'utilisateur et un mot de passe, une deuxième preuve de l'identité. Il peut s'agir d'une liste TAN ou d'un jeton d'identification tel qu'une smartcard qui est exclusivement en possession du détenteur du compte.
- Utilisez un logiciel de sécurité adéquat (antivirus, pare-feu, etc.) et maintenez-le à jour.

Recherchez activement sur Internet les données qui sont sauvegardées à votre sujet et vérifiez si elles sont correctes. A l'adresse https://haveibeenpwned.com, vous pouvez vérifier si votre adresse e-mail ou votre compte d'utilisateur a été compromis.

Published under the copyright license "Attribution – Non-Commercial – NoDerivatives 4.0". No commercial reuse without permission. See: http://emh.ch/en/services/permissions.html