Baloise
SCOUTS
DIGITAUX

Cyber Security Guide – pour les personnes privées

Nous vous montrons la voie dans la jungle numérique.

www.baloise.com/digitale-pfadfinder

Baloise
Group

À propos des Scouts Digitaux

La troupe des Baloise Scouts Digitaux réunit des collaborateurs motivés et impliqués. Ambas-sadeurs de la numérisation, ils vous offrent leur aide pour vous y retrouver dans la jungle numérique. L'organisation des Baloise Scouts Digitaux est une collaboration entre GroupIT et Public Affairs.

Objet et but des Scouts Digitaux
Les Baloise Scouts Digitaux apportent une contribution volontaire dans le cadre de la respon-sabilité sociale de l'entreprise, car les besoins de la société vont au-delà des prestations de sécurité. Les collaborateurs de la Bâloise disposent d'un vaste savoir-faire qui est mis à la disposition de la société en plus des prestations de services liées à notre activité.

Une séance d'information sur la cybersécurité vous intéresse? Contactez-nous par e-mail:
pfadfinder@baloise.com

Introduction

Cette brochure est destinée à vous aider à vous informer sur les dangers et les risques de l'utilisation quotidienne d'Internet à titre privé. Elle explique ensuite les bases de la cybersécu-rité et vous fournit des lignes directrices de prévention permettant d'éviter les cyberincidents.

Les risques de cybersécurité existent sous de nombreuses formes et peuvent causer des dommages importants, voire désastreux. À domicile comme au bureau, la plus grosse fai-blesse de la sécurité informatique est et reste toujours l'homme lui-même. Mais à travers une compréhension claire des risques et des conséquences de nos propres actions, cette faille peut toutefois être considérablement réduite.

Les principaux termes brièvement expliqués

Ingénierie sociale
Le mode opératoire consiste à manipuler des personnes afin de les inciter à adopter un cer-tain comportement – par exemple, abuser de leur crédulité pour les amener à révéler des informations confidentielles. En faisant aussi appel à la serviabilité de leurs victimes, les «social engineers» tentent de parvenir à des données sensibles.

Hameçonnage
Tentative d'accéder aux données personnelles d'un utilisateur Internet au moyen de pages web, d'e-mails, ou de messages falsifiés dans le but de lui nuire (p. ex. vol de données ou de valeurs pécuniaires). Il s'agit d'une forme d'ingénierie sociale.

Cyberharcèlement
Terme générique désignant les formes de calomnie et de harcèlement d'autres personnes et entreprises par le biais d'Internet ou d'appareils mobiles. Le vol d'identités, qui a par exemple pour but de conclure des affaires ou de faire des déclarations au nom d'un tiers, en fait aussi partie. Il s'agit là encore d'une forme d'ingénierie sociale.

Maliciels
Terme générique désignant les programmes qui accomplissent des fonctions indésirables et dommageables. Le maliciel ne se propage souvent pas de lui-même, mais sollicite l'utilisation d'un programme hôte afin de conduire l'utilisateur à l'installer. Les maliciels les plus connus sont les chevaux de Troie, les logiciels espions et les rançongiciels.

Rançongiciels
Aussi appelés ransomware ou Trojans encodeurs, ce sont des logiciels malveillants avec lesquels un intrus peut empêcher d'accéder à des données et de les utiliser, ou encore em-pêcher l'accès au système informatique tout entier. L'objectif est d'exiger une rançon pour obtenir le déchiffrage ou le déblocage. En 2017, «WannaCry» et «NotPetya» ont attiré l'attention aux quatre coins du monde en paralysant complètement des hôpitaux et des entre-prises de logistique, entre autres.

Déni de service distribué (DDoS)
Blocage des services informatiques exposés à Internet (site web, boutique en ligne ou forum), provoqué par une énorme quantité de demandes. Ce blocage empêche l'utilisation du service informatique visé. Ce genre d'attaque peut être causé par des surcharges involontaires ou une attaque ciblée. Il s'agit d'une forme de chantage de plus en plus courante à l'ère du com-merce en ligne.

Sensibilisation
Gestion des mots de passe et sécurité

Les mots de passe ne devraient être écrits nulle part, ni communiqués à un tiers. L'authentification à plusieurs facteurs est un moyen simple et efficace pour renforcer la sécu-rité d'un compte. Un SMS est par exemple envoyé au numéro de téléphone portable enregistré de l'utilisateur qui reçoit un code à chiffres pour continuer l'identification. Pour chaque compte, il faudrait utiliser des mots de passe différents qui ne se ressemblent pas. Il faut partir du principe que l'on peut perdre les mots de passe, c'est pourquoi il faut les modifier régulièrement. À cet égard, il est important de ne pas remplacer uniquement un chiffre ou une lettre, et de choisir au contraire un mot de passe entièrement nouveau.

Si l'on soupçonne une utilisation abusive d'un compte, il est important de changer immédiate-ment le mot de passe s'y rapportant.

Gestionnaires de mots de passe (password-vaults)

Les gestionnaires de mots de passe, également appelés «password-vaults», simplifient la création et la mémorisation de mots de passe nouveaux ou existants. Ces applications per-mettent de générer un mot de passe sûr et de le stocker en le reliant à un compte. L'application est elle-même protégée par un mot de passe principal complexe ou par la recon-naissance faciale ou d'empreinte sur un smartphone. Ainsi, vous n'avez que le mot de passe principal à mémoriser et vous pouvez consulter de façon très simple tous les autres mots de passe. Voici quelques bons exemples de gestionnaires de mots de passe: SecureSafe, 1Password et Keeper Security.

Check-list pour la sécurité des mots de passe

- ☐ Au moins 8 caractères
- ☐ Minuscules et majuscules
- ☐ Chiffres et caractères spéciaux
- ☐ Pas de séries de lettres figurant dans un dictionnaire
- ☐ Jamais utilisé auparavant

Conseil

Si vous ne pouvez pas utiliser de gestionnaire de mots de passe, les moyens mnémotech-niques ou les phrases mots de passe peuvent vous aider à créer des mots de passe ou à les mémoriser plus facilement. Il s'agit en l'occurrence de phrases simples dans lesquelles on utilise l'initiale de chaque mot pour former un mot de passe.

Exemple:

→ Phrase mot de passe : Mon fil est né en février 1994, il va avoir 26 ans cette année.

→ Chaque première lettre ou chiffre dans l'ordre en respectant les minuscules et majuscules:

Mon fil est né en février 1994, il va avoir 26 ans cette année.
→ Mot de passe: **Mfenef94$iv a26aca**

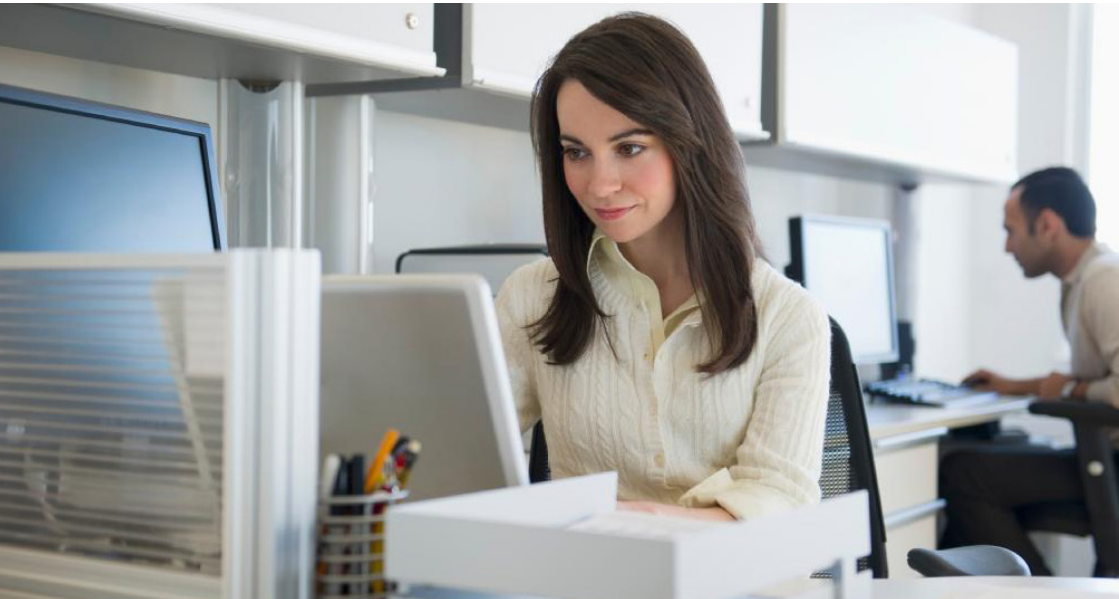
Ingénierie sociale
Scénarios et conduite à tenir

Vous pouvez être victime d'ingénierie sociale au cours d'un entretien direct, en ligne ou au téléphone. Les exemples de scénarios suivants devraient vous aider à être attentif à certains schémas:

Situation: un prince nigérian vous contacte par e-mail en vous expliquant qu'il souhaite livrer en Suisse une quantité d'or représentant plusieurs millions de francs. Vous devez intervenir en tant qu'intermédiaire et vous pourrez conserver une certaine part du chiffre d'affaires.

→ Conduite recommandée: il s'agit d'un classique qui, malheureusement, fonctionne encore trop souvent. Si un inconnu vous propose via Internet un profit intéressant, vous pouvez être sûr qu'il s'agit d'une escro-querie. Ne répondez pas à ce message et supprimez-le immédiatement.

Situation: une personne avec qui vous avez fait connaissance en ligne, mais que vous n'avez pas en-core rencontrée personnellement, vous envoie un message en vous parlant de problèmes fami-



liaux et en vous expliquant qu'il ou elle a besoin d'argent pour se rendre dans son pays d'origine. Cette personne demande souvent de lui acheter des avoirs sur Mastercard Prepaid.

→ Conduite recommandée: rompez tout contact avec cette personne. Il est fort probable qu'il ne s'agisse pas de la personne qui s'est présentée sur le portail en ligne, et peut-être même pas d'une personne du sexe indiqué. Bloquez-la et signalez-la aux administrateurs du portail pour qu'elle soit retirée de la plateforme.

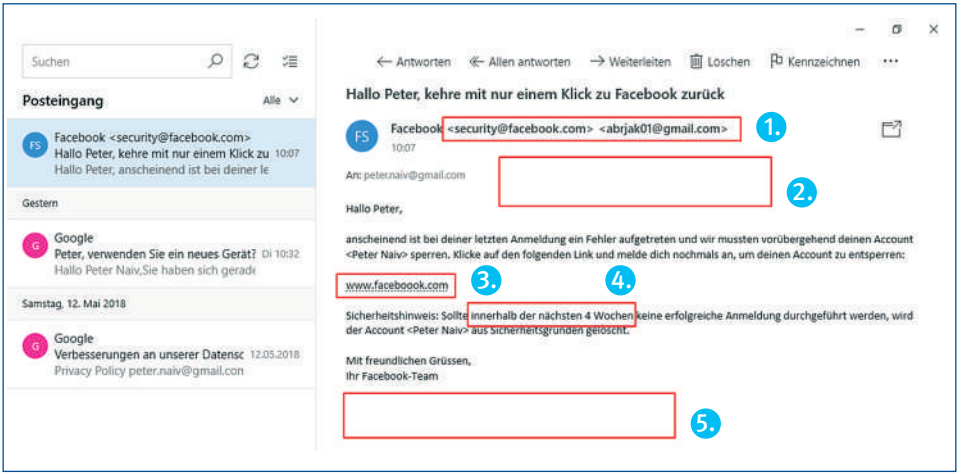
Situation: une personne vous contacte par téléphone en se présentant comme un agent de la helpdesk d'un constructeur de matériel (HP, Dell, Apple, etc.) et en vous indiquant que votre appareil présente un problème. Il vous demande ensuite de lui communiquer diverses données personnelles ainsi que des détails sur votre appareil et votre connexion Internet.

→ Conduite recommandée: ne communiquez jamais de données détaillées vous concernant ou concernant votre appareil lorsque l'on vous appelle par téléphone, et raccrochez. Les constructeurs de matériels n'ont pas la possibilité de savoir automatiquement si et comment l'appareil que vous avez acheté fonctionne. En cas de problème, c'est à vous d'appeler la helpdesk du constructeur.

Situation: une personne se présentant en tant qu'administrateur intervient dans le chat de votre jeu en ligne et vous informe que votre compte est corrompu. Afin de réparer le compte avant que vous ne perdiez de précieuses données de jeu, il a besoin de votre mot de passe et de l'adresse e-mail que vous avez utilisée pour vous inscrire au jeu.

→ Conduite recommandée: ignorez cette personne puis bloquez-la ou signalez-la, si possible. Aucun administrateur de jeu n'interviendrait dans un chat pour vous parler de problèmes de compte. Ces problèmes sont toujours traités par e-mail. Normalement, l'éditeur du jeu vous informe toujours qu'aucun de ses administrateurs ne vous demandera de communiquer des données personnelles par chat. Ignorez également tous les messages envoyés par chat vous proposant à un prix intéressant des montants importants dans la «monnaie du jeu». Là encore, il s'agit toujours d'escroqueries.

Hameçonnage
Scénario et conduite à tenir



L'e-mail sur la page de droite explique avec un exemple simple à quoi l'on peut reconnaître un e-mail de hameçonnage et la conduite à suivre dans une telle situation.

Caractéristiques distinctives (boîtes rouges) de haut en bas:

1. L'expéditeur indiqué a deux adresses e-mails et la seconde ne ressemble vraiment pas à celle d'un collaborateur Facebook.
2. Il manque le logo Facebook. L'ensemble de l'e-mail n'a pas le formatage habituel de Face-book.
3. Le lien mentionné vers Facebook contient un «o» de trop. De plus, le lien ne montre aucun signe pour rediriger l'utilisateur vers une ouverture de session ou une page de déverrouillage.

4. L'e-mail semble urgent. Une menace sous forme d'une suppression de compte est aussi ex-primée dans la même phrase.

5. Les typiques disclaimer et remarques sur la protection des données à la fin de l'e-mail sont absents. Les moyens possibles pour prendre contact avec l'assistance de Facebook ne sont pas indiqués. Si le compte doit vraiment être supprimé dans les plus brefs délais, c'est là que vous trouveriez les données de contact.

D'autres caractéristiques typiques des e-mails de hameçonnage peuvent être:

→ une formulation impersonnelle;
→ - une orthographe incorrecte et des problèmes d'accentuation;
→ - l'utilisation d'une langue inhabituelle pour le pays (p. ex. l'anglais alors que le service est utili-sé en français);
→ - une mise en page non homogène dans l'e-mail.

Faits et chiffres:

45% des internautes cliquent sur les liens dans les e-mails d'expéditeurs inconnus.
92 % des cyberattaques commencent par un e-mail de hameçonnage.

Comment procéder avec des e-mails de hameçonnage?

Les e-mails de hameçonnage ne sont pas toujours clairement identifiables. Si l'on soupçonne toutefois qu'un e-mail reçu est un e-mail de hameçonnage, il est possible de procéder comme suit:

→ Supprimer l'e-mail; s'il s'agit effectivement d'un message important, un véritable service en ligne se manifestera de nouveau.
→ Vérifier manuellement (sans passer par le lien indiqué dans l'e-mail) le statut du profil ou du service.
→ Appeler l'assistance clientèle de l'expéditeur et demander des informations. Le numéro de l'assistance clientèle d'un prestataire de services se trouve la plupart du temps très rapidement sur Google.

Notez bien qu'une entreprise sérieuse n'utiliserait jamais un simple e-mail pour vous informer de la suppression de votre compte. Les établissements financiers et d'assurance, en particu-lier, prendraient tout d'abord contact avec vous par téléphone ou par courrier postal en cas de problème sur votre compte.

Hameçonnage SMS

L'hameçonnage peut également se produire via un SMS sur votre téléphone mobile. Vérifiez lors de la réception d'un SMS avec un lien, à reconnaitre une tentative d'hameçonnage:

- → Vérifier nom et numéro de l'expéditeur
- → Vérifier l'orthographe du message
- → Regarder le lien (par ex. nom de l'entreprise correctement orthographiée)
- → En cas de doute contacter le service client de l'entreprise par téléphone ou par mail.

Protection contre les rançongiciels
et réaction en cas d'incident

Un rançongiciel peut parvenir sur votre système par divers moyens et vous causer des dommages en cryptant vos données. Pensez aux mesures suivantes pour éviter cette forme de chantage:

→ Prudence avec les e-mails, en particulier en ouvrant des pièces jointes. Le rançongiciel est principalement diffusé par e-mail et se propage lorsque vous cliquez sur des liens et que vous téléchargez des pièces jointes sur votre système. Confiez impérativement à votre protection antivirus le soin d'examiner les pièces jointes provenant d'expéditeurs inconnus.

→ Prudence avec les supports de stockage tels que les clés USB et les disques durs nomades. En particulier si vous ne connaissez pas le précédent utilisateur du support de stockage et que vous n'êtes pas sûr de savoir ce qui se trouve dessus, vous ne devriez pas le connecter à votre système.

→ Maintenez toujours vos systèmes à jour. Les nouvelles versions des logiciels d'exploitation apportent souvent des améliorations portant sur la sécurité de l'information. Les mises à jour de votre programme antivirus aussi contiennent des améliorations dans la détection et la lutte contre les virus. Elles devraient toujours être effectuées.

Sachez que les rançongiciels sont souvent programmés de façon à se propager à travers le réseau infecté. Cela signifie, par exemple, que tous les appareils connectés à votre réseau Wi-Fi sont les prochaines victimes potentielles du rançongiciel.

→ Utilisez par conséquent une solution de sauvegarde pour tous les appareils de votre foyer, et effectuez régulièrement des copies de sécurité de vos données et de celles de vos coloca-taires.

En cas d'incident?

→ Ne payez pas la somme exigée! Souvent, la somme augmente par la suite, sans pour autant que vos données soient décryptées.

→ Tournez-vous vers un spécialiste et essayez de restaurer votre système avec une sauve-garde ayant été faite avant l'incident.

Autres lignes directrices de prévention importantes

Informer les membres de la famille et les colocataires
Lorsque plusieurs appareils connectés à Internet et plusieurs utilisateurs se trouvent sous le même toit, informez ces derniers des risques liés à Internet et échangez avec eux. Les en-fants et les jeunes en savent souvent plus sur Internet que l'on ne pense. Il est par consé-quent recommandé de convenir ensemble d'une solution commune et de règles de comportement.

Sécuriser les données – faire des back-up
Le risque de perdre vos données n'existe pas uniquement dans le cas d'une cyberattaque. D'autres facteurs externes, tels qu'un incendie, des dégâts d'eau ou la détérioration physique de l'appareil, peuvent également entraîner une perte de données.
Créez donc régulièrement des copies de sécurité de vos données, les dénommés «back-up». Pour ceci, des programmes plus ou moins bons, et plus ou moins chers sont proposés. Il est en outre important de vérifier régulièrement si les données sauvegardées peuvent être correctement restaurées. À noter également que les back-ups ne doivent pas être conservés sur le même appareil et au même endroit que les données originales. Utilisez pour cela un disque dur externe ou une solution de sauvegarde qui enregistre vos données dans un cloud. Si vous utilisez une solution de sauvegarde dans le cloud, sachez toutefois que selon l'endroit où se trouve l'entreprise, les lois sur la protection des données sont différentes des lois suisses.

Nous recommandons également l'installation d'un pare-feu qui vous protège des attaques extérieures, et d'un antivirus qui contrôle régulièrement votre système et les données qui s'y trouvent.
La plupart des antivirus, pare-feu et programmes de back-up offrent une version d'essai ou sont pour certains disponibles gratuitement. Prenez par conséquent le temps de tester plu-sieurs programmes et choisissez une solution qui corresponde à votre budget et à vos exigences, tant au niveau du prix que des prestations.

Mise à jour des systèmes d'exploitation et des programmes
Installez rapidement les mises à jour d'exploitation et de sécurité régulières pour votre sys-tème d'exploitation et vos programmes. Ces «correctifs» permettent de rectifier des erreurs et des failles de sécurité connues, et de renforcer ainsi la sécurité de toutes les fonctions.
Tous les systèmes d'exploitation et programmes pour ordinateur et smartphone ne sont pas sans faille. Les concepteurs des maliciels tirent souvent parti de ces failles pour accéder à l'ordinateur ou au smartphone. C'est pourquoi il est intéressant d'utiliser des solutions d'antivirus et de pare-feu en plus des services de sécurité standard de votre système d'exploitation (par ex. «Windows-Defender»).

Faire preuve de bon sens
Lorsque vous surfez et effectuez des opérations sensibles sur Internet, faites toujours preuve de bon sens.

Pour d'autres lignes directrices de prévention, des informations sur la cybersécurité ou en-core d'intéressants piratages en direct, participez aux séances d'information et aux présenta-tions des Baloise Scouts Digitaux.

Le piratage est répréhensible
Toutes les sortes de cyberattaques sont interdites par la loi.

Soutien de l'État
L'État met à disposition depuis 2010 la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) sur **www.melani.admin.ch**. Vous y trouverez des informations sur les risques et mesures actuels, ainsi qu'un formulaire de déclaration d'incident.

Have I Been pwned?
Le site Internet «Have I Been pwned» (HIBP) réunit et analyse des «data dumps», autrement dit des vidages de mémoires qui suite à des violations de données ont été mis en ligne par des pirates informatiques. HIBP offre à l'utilisateur la possibilité de vérifier si dans cette multi-tude de données utilisateurs divulguées et par conséquent menacées, se trouve sa propre adresse e-mail ou son nom d'utilisateur. Il est également possible d'intégrer une fonction qui informe l'utilisateur par e-mail si ses propres données ont été divulguées dans une violation de données. Ou encore de chercher des mots de passe déjà publiés. C'est pourquoi il est important d'utiliser plusieurs mots de passe car les mots de passe ayant été divulgués dans une violation de données sont vendus sur Internet et ne devraient par conséquent plus être utili-sés.
https://haveibeenpwned.com

Baloise Group
Aeschengraben 21
CH-4002 Basel
pfadfinder@baloise.com

www.baloise.com

000.1039f 2.20 500