La sécurité en ligne

Manuel

Summary

1.Introduction

1.1 Bienvenue

Bienvenue dans « la sécurité en ligne ».

Ce cours montrera dans quelle mesure la sécurité des utilisateurs en ligne est fondamentale pour gérer la sécurité informatique d'une entreprise.

1.2 La sécurité des utilisateurs en ligne

Le contexte actuel

Les attaques par ingénierie sociale, c'est-à-dire l'exploitation programmée des habitudes et des relations sociales, ne représentent rien de nouveau. Les fraudes ainsi que les personnes manipulatrices ont toujours existé.

Au cours des dernières années, les progrès technologiques ont amélioré la communication ainsi que le partage des informations. Les attaques sont ainsi devenues encore plus faciles et immédiates.

La sécurité informatique au quotidien

Dans certaines situations de la vie de tous les jours, nous ignorons souvent les risques liés à la sécurité informatique. Par exemple, le fait de partager des informations personnelles ou confidentielles avec des personnes mal choisies peut représenter un risque, quel que soit le cadre :

- dans une pièce, sur internet, sur les médias sociaux
- chez soi ou au travail

Protéger les informations d'une personne ainsi que son identité numérique est une manière de se protéger et d'augmenter le niveau de sécurité en entreprise.

Donc, n'oubliez pas :

- la sécurité informatique concerne des situations dans la vie de tous les jours
- vous pouvez protéger votre entreprise en vous protégeant vous-même

1.3 La structure du cours

Objectifs et plans du cours

L'objectif de ce cours est de sensibiliser aux situations qui comportent un risque pour vous et pour la sécurité de votre entreprise et vous rappeler les règles de comportement à suivre.

Le cours se compose de 7 modules de formation :

2. Les attaques par ingénierie sociale

2.1 Les objectifs de ce module

Les objectifs

Ce module vous exposera les attaques par ingénierie sociale, qui sont à la base des risques liés aux personnes. Nous présenterons les risques principaux liés à ces attaques et nous les approfondirons dans les modules successifs.

2.2 Vue d'ensemble

Les caractéristiques d'une attaque par ingénierie sociale

Aujourd'hui, les attaques contre les systèmes des entreprises ne visent plus les contre-mesures de sécurité physique ou technologique. Elles exploitent la possibilité de manipuler le comportement des utilisateurs liés à la cible qu'elles désirent viser.

Cela signifie que toute personne ayant accès aux biens ou aux informations de l'entreprise peut être victime d'une attaque par ingénierie sociale visant à récupérer des informations critiques, confidentielles ou potentiellement utiles à étendre l'attaque, ou qui permettent tout simplement au hacker de percer les défenses informatiques.

Donc, soyez attentifs :

- vous pourriez vous aussi faire l'objet d'une attaque !
- vous pourriez vous aussi fournir des informations ou les droits d'accès au système de votre entreprise.

Comment pouvez-vous faire l'objet d'une attaque?

Une attaque par ingénierie sociale typique vous manipulera afin que vous fassiez quelque chose de potentiellement dangereux, comme divulguer vos données d'accès ou visiter un site web malveillant, en comptant sur votre curiosité, votre peur, votre imprudence, voire sur vos habitudes.

Ces attaques peuvent être menées en utilisant différentes techniques, c'est pourquoi il est important de les connaître. Jetons un œil sur quelques exemples :

- interaction directe avec des personnes peu fiables
- phishing
- installation de logiciel avec des fonctionnalités cachées
- s'inscrire à des services en utilisant toujours les mêmes données d'accès
- partager des contenus par l'intermédiaire des médias sociaux
- fausses contre-mesures de sécurité proposées par votre PC (chevaux de Troie qui se font passer pour des mises à jour de logiciel)

À quoi devriez-vous faire attention ?

Il existe différents scénarios d'attaque et cela peut être une source d'inquiétude. Cependant, il n'est pas si difficile de se protéger. Jetons un œil sur certaines choses auxquelles vous devez être vigilant.

Tout d'abord, souvenez-vous de rester vigilant à tout moment et en toute situation de la vie de tous les jours :

- quand vous bavardez au bar avec vos collègues
- quand vous êtes devant votre ordinateur
- quand vous téléphonez

Ensuite, n'oubliez pas que toute information est à la base de chaque attaque. C'est pourquoi, afin d'éviter de transmettre ces informations à des personnes dangereuses, il faut toujours rester attentif au contexte de la communication :

- avec qui êtes-vous en train de communiquer
- le lieu physique ou virtuel où la communication se déroule
- comment ces personnes vous demandent ces informations.

Rappelez-vous, les environnements communs aussi peuvent être la cible des hackers ! Il est important de savoir reconnaître quelles actions apparemment anodines peuvent dissimuler des pièges, par exemple :

- naviguer sur un site web inconnu
- installer un logiciel sur votre PC ou une application sur votre mobile
- partager des informations personnelles sur les médias sociaux

Tous les gens d'Eni doivent aider activement à maintenir la sécurité de l'entreprise. Rapporter toute cyber-attaque présumée ou effective à votre supérieur ou au service de l'entreprise compétent en la matière.

Dans les prochains modules, nous analyserons de plus près les risques et les points importants liés aux attaques traditionnelles et technologiques. Pour l'heure, il est important de se souvenir qu'il est essentiel de rester vigilant. La précipitation peut vous conduire à faire de graves erreurs, telles que celles que nous allons voir dans les pages suivantes.

2.3 Erreurs fréquentes

Quelques points importants

Les erreurs commises dans ces deux épisodes soulignent l'importance de prêter la plus grande attention au contenu de la communication et aux endroits où vous partagez ces informations.

En résumé, souvenez-vous qu'il est très important de :

- choisir quelles sont les informations que vous pouvez partager
- étudier l'endroit où vous vous trouvez et si quelqu'un peut intercepter votre conversation

3. La sécurité des informations dans la vie de tous les jours

3.1 Les objectifs de ce module

Les objectifs

Dans ce module, nous analyserons les éléments qui menacent la sécurité des informations, au bureau, dans les lieux publics et à la maison. Nous soulignerons ensuite certaines règles de comportement appropriées.

En effet, la technologie n'est pas la seule menace à la sécurité des informations. Dans la vie de tous les jours, il existe de nombreuses situations dans lesquelles un comportement apparemment anodin peut devenir un risque pour vous-même et pour l'entreprise pour laquelle vous travaillez.

3.2 Au bureau

Ce qui peut arriver quand vous êtes au bureau

Nous supposons tous que le bureau est un endroit fiable avec la seule présence de personnes de confiance. C'est effectivement généralement le cas ; cependant, certaines précautions éviteront l'utilisation incorrecte des informations que vous détenez.

Par exemple, quelqu'un pourrait :

- vous observer quand vous entrez votre mot de passe ou lire ce que vous avez écrit sur le post-it que vous avez mis sur votre écran
- lire le fichier que vous avez ouvert sur votre ordinateur
- écouter vos appels téléphoniques
- prendre vos documents de l'imprimante
- fouiller dans les papiers que vous avez jetés à la poubelle pour trouver des documents intéressants

Restez toujours vigilant quant à ce que vous êtes en train de faire et aux personnes présentes autour de vous. Réfléchissez à cela :

- quand vous parlez d'informations confidentielles au bureau, êtes-vous sûr que seules les personnes autorisées peuvent vous entendre ?
- quand vous lisez un e-mail ou un document ou que vous entrez votre mot de passe, vous assurez-vous que personne derrière vous ne peut vous voler ces informations ?
- quand vous imprimez un document, le retirez-vous toujours de l'imprimante immédiatement ou le laissez-vous parfois sans surveillance ?
- quand vous décidez de jeter un document imprimé qui contient des informations cruciales, prenez-vous soin de le détruire ?

Ce qui peut arriver quand vous quittez le bureau

Il est important de prendre certaines précautions pour protéger les informations quand vous quittez le bureau, car quelqu'un pourrait y avoir accès quand vous êtes absent. Quelques simples mesures peuvent aider :

- fermez vos tiroirs à clé

- ne laissez pas de documents confidentiels, de dispositifs de stockage de données (clés USB, CD, disques durs externes) ou de dispositifs (téléphones mobiles, smartphones, tablettes) sur votre bureau
- assurez-vous d'avoir verrouillé votre ordinateur

3.3 Dans les lieux publics

Les lieux remplis de monde et la présence d'étrangers

Le bureau n'est pas toujours un lieu fiable, les lieux publics encore moins.

Quand vous êtes dans le métro, à l'arrêt de bus, dans un bar, dans le train, prenez toujours en compte la présence d'étrangers et prenez des mesures pour protéger la confidentialité.

Par exemple :

- introduire votre mot de passe dans votre mobile quand vous êtes dans un lieu rempli de monde peut être dangereux si vous ne regardez pas derrière vous. Quelqu'un pourrait jeter un coup d'œil et voler votre identité numérique
- quand vous parlez avec quelqu'un, prenez soin d'observer les personnes qui pourraient vous écouter. Certaines personnes peuvent voler des informations confidentielles et provoquer ainsi des situations embarrassantes. Imaginez : vous êtes dans le train, en train de bavarder avec un ami et vous commencez à critiquer un fournisseur ou un client, pour découvrir ensuite que la personne assise à côté de vous travaille dans la même entreprise.

Précautions lors de l'utilisation de dispositifs de l'entreprise

L'utilisation de dispositifs professionnels dans des lieux publics demande d'adopter des précautions supplémentaires.

Par exemple, vous êtes à l'aéroport ou dans un autre lieu public et vous avez besoin de vous connecter à internet par l'intermédiaire d'un réseau Wi-Fi. Il est important de vérifier à quel réseau vous êtes en train de vous connecter. Se connecter à internet à partir d'un réseau non sécurisé signifie entrer dans un environnement ouvert à tous, et risquer que vos données personnelles soient interceptées par des hackers.

3.4 À la maison

Accès aux services de l'entreprise

Travailler depuis son domicile en utilisant ses propres dispositifs ou ceux de l'entreprise pour interagir avec les services de l'entreprise peut présenter des risques, étant donné qu'une connexion internet à domicile n'offre pas le même niveau de protection que le réseau de l'entreprise.

Cette connexion n'est pas contrôlée par un système de prévention contre les cyber-attaques. De plus, votre ordinateur personnel ne présente pas la même configuration que celui que vous avez au bureau.

C'est pourquoi vous devez rester extrêmement prudent quand vous accédez aux services de l'entreprise en dehors du bureau. Les conseils suivants peuvent se révéler très utiles :

- si vous vous connectez à des services de l'entreprise depuis votre domicile ou des postes de travail partagés :

    - ne cochez pas l'option « se souvenir de moi »
    - ne téléchargez pas de fichiers ou de documents confidentiels relatifs à l'entreprise sur votre ordinateur personnel
- n'installez pas d'outils de l'entreprise sur votre ordinateur personnel
- ne stockez pas de données privées relatives à l'entreprise sur des serveurs cloud publics (par exemple Google Drive, Cloud, etc.)
- ne transférez pas de données privées relatives à l'entreprise par l'intermédiaire d'applications en ligne (par exemple Wetransfer, Dropbox), quelle qu'en soit la taille

3.5 Protégez votre entreprise en vous protégeant vous-même

Précautions à adopter

Bien, ce module est maintenant terminé. Résumons ce que nous avons appris.

Dans ce module, nous avons exposé certaines règles de comportement à suivre dans la vie de tous les jours, en particulier quand nous interagissons avec d'autres personnes.

Ces règles se basent sur les recommandations spécifiques d'Eni :

- respecter le principe de besoin de savoir, selon lequel seules les personnes qui ont besoin de certaines informations pour accomplir leurs tâches peuvent y avoir accès
- seules les personnes autorisées devraient avoir accès à ces informations
- protégez vos identifiants d'accès à votre poste de travail

D'après ces recommandations :

- nous avons vu quelques exemples qui soulignent combien il est important de rester vigilant quant au contexte et à la situation dans laquelle vous vous trouvez ainsi qu'aux personnes qui vous entourent
- nous avons remarqué combien il peut être dangereux de laisser des objets ou des documents sans surveillance ou de laisser le libre accès à votre bureau ainsi qu'à vos outils professionnels même lorsque vous n'êtes pas présent
- nous avons souligné l'importance d'être particulièrement vigilant lorsque vous avez accès aux services de l'entreprise en dehors du réseau de l'entreprise, qui ne possède pas la protection ni les contre-mesures mises en œuvre au sein de l'entreprise

Si vous désirez en savoir plus à propos de ces règles de comportement que tous les gens d'Eni doivent respecter en matière de création, partage, réception, reproduction, protection et destruction des informations, veuillez faire référence à :

- la politique en matière de gestion des informations
- les lignes directrices du système de gestion en matière d'abus de marché et de communication externe
- les procédures « Corporate Information Protection » et « Assigning criteria and utilization rules of ICT resources for individual use »

4. Internet et logiciel

4.1 Les objectifs de ce module

Les objectifs

Bienvenue dans le quatrième module de ce cours.
Dans ce module, nous analyserons les risques principaux quand vous naviguez sur internet ou que vous installez un logiciel sur votre ordinateur ainsi que sur des dispositifs mobiles.
L'usage de la technologie fait partie intégrante de la vie de tous les jours. La facilité avec laquelle la plupart d'entre nous l'utilise mène souvent à faire des choses qui, par inadvertance, peuvent mettre en danger la sécurité de nos dispositifs, et par conséquent, le réseau de l'entreprise.

4.2 Naviguer sur internet

Comment pouvez-vous mettre votre ordinateur en péril lorsque vous naviguez sur internet

Internet est un phénomène aux formes multiples mais qui devient de moins en moins sûr.
La sécurité peut être mise en péril en naviguant sur des sites web douteux et en agissant de manière à déclencher des risques.
Les sites malveillants sont souvent difficiles à identifier. C'est pourquoi il est important de naviguer sur des sites web « connus », par exemple les sites web que vous avez toujours utilisés ou ceux qui sont bien réputés.
Malgré les configurations des ordinateurs et l'installation de logiciels de protection, quand vous naviguez, vous rencontrez souvent des messages qui devraient vous alerter, comme :

- sondages pop-up, produits, publicités
- rappels soudains de mise à jour de logiciel
- demandes d'installation de barres et d'extensions sur votre navigateur
- messages vous communiquant que votre ordinateur est vulnérable

Ces évènements ainsi que d'autres sont habituellement associés à un avertissement qui vous incite à installer quelque chose de douteux. Si, après avoir cliqué, vous remarquez que votre ordinateur est plus lent ou qu'il a tendance à se bloquer et que l'écran devient bleu, alors, quelque chose s'est passé. Il faut que vous le fassiez contrôler avant de pouvoir le réutiliser.
Donc, attention : ne cliquez sur aucune fenêtre ou message sans savoir de quoi ils parlent !

4.3 Logiciel douteux ou piraté

Pourquoi dire NON à un logiciel piraté

Bien que cela soit une pratique illégale, installer gratuitement un logiciel piraté non autorisé, non original, à partir de sites douteux était une pratique fréquente par le passé.
Aujourd'hui, bien qu'il existe des plateformes légales qui tentent de résoudre ce problème par l'intermédiaire de la distribution de masse en offrant des produits à des prix raisonnables, le piratage reste répandu et affecte principalement les logiciels coûteux.
Pour éviter ces risques et pour protéger la sécurité informatique de votre entreprise, il est interdit de télécharger tout logiciel au travail.
Chez vous aussi, soyez prudent en cas de logiciel payant offert gratuitement.

Logiciel cracké

Un logiciel non autorisé est copié de manière illégale en utilisant un logiciel invasif (crack), qui modifie l'application d'origine pour désactiver son système de protection, ou un logiciel qui génère une activation ou des clés d'activation, permettant de les utiliser.
Ces types de logiciel représentent souvent la source principale d'installation de logiciels malveillants, qui peuvent endommager l'ensemble du système d'exploitation.
De plus, les sites qui offrent des logiciels crackés ou des outils de cracking peuvent être malveillants et infecter votre ordinateur quand vous les consultez.

Les risques du logiciel libre

De plus, les logiciels d'installation libres contiennent souvent d'autres logiciels, qui installent, sciemment ou non :

- des barres de recherche pour navigateur, qui peuvent intercepter des informations personnelles ou interférer avec le contenu de la navigation
- un logiciel supplémentaire, qui transmet des informations ou des contenus sur l'ordinateur

Souvenez-vous que tout programme ou toute extension que vous installez met votre ordinateur en péril. Assurez-vous qu'il ou elle provient de sources fiables.

4.4 Applications mobiles

Risques

On est bien conscient que les ordinateurs peuvent faire l'objet d'une attaque. Toutefois, les menaces à l'encontre des dispositifs mobiles restent largement sous-estimées.
Que se passe-t-il si vous sous-estimez les menaces à l'encontre de vos dispositifs mobiles ?
Tout d'abord, il est important de souligner que tous les téléphones peuvent faire l'objet d'une attaque en exploitant :

- des applications malveillantes téléchargées à partir de sites de distribution officiels et parfois aussi à partir de sites non officiels, bien qu'ils soient régulièrement contrôlés en contournant les mesures de contrôle. Une fois installées, elles peuvent permettre l'accès non autorisé à des données personnelles et à des fonctions du téléphone
- la vulnérabilité du système en utilisant des navigateurs (sur ordinateurs) ou en activant des canaux de communication, par exemple connexions Bluetooth, téléchargement de fichiers, scannérisation des codes QR
- l'interception de communications, notamment si vous vous connectez à n'importe quel réseau Wi-Fi, même si ouvert

L'étendue du danger dépend du dispositif et de sa configuration.
Lors de l'achat d'un dispositif mobile, les systèmes d'exploitation (par exemple Android ou Apple iOS) limitent la liberté des utilisateurs de télécharger des applications ou de changer de configuration.
Si vous désirez personnaliser votre dispositif et contourner ces restrictions, vous devez débloquer votre téléphone. Cette procédure est appelée enracinement sur Android et jailbreaking sur iOS et vous permet de contourner les restrictions qui vous empêchent d'accéder aux zones les plus profondes du système.

Souvenez-vous que les risques d'atteinte à la sécurité augmentent quand vous débloquez un dispositif mobile, car les contre-mesures du système sont éliminées.

Donc, attention :

- un téléphone n'est pas plus fiable qu'un ordinateur. Soyez attentif à ce que vous installez et où vous naviguez
- ne débloquez pas votre téléphone dans le seul but d'installer des applications gratuites ou de supprimer des publicités. Économiser quelques centimes pourrait se solder par un coût bien plus élevé

Quelles précautions adopter ?

Comment pouvez-vous contrôler ce que vous installez sur votre téléphone ?
Il existe certaines mesures de base, comme éviter de débloquer votre téléphone. En général, il s'agit de faire preuve d'attention et de bon sens et de respecter les caractéristiques de sécurité du système d'exploitation de votre dispositif mobile.
Découvrez les aperçus pour en savoir plus à propos des caractéristiques des systèmes d'exploitation Android et iOS et les précautions à adopter.
Mais rappelez-vous, peu importe le système d'exploitation que vous utilisez, vous devriez toujours utiliser vos dispositifs mobiles avec attention.

4.5 Protéger votre entreprise en vous protégeant vous-même

Précautions à adopter

Bien, ce module est maintenant terminé. Résumons ce que nous avons appris.
Dans ce module, nous avons identifié quelques règles de comportement à suivre quand vous naviguez sur internet ou que vous installez un logiciel. Nous avons appris que :

- le seul fait de jeter un œil sur un site peut mettre votre ordinateur en péril. Donc, soyez prudent quant aux sites sur lesquels vous naviguez. Ne vous fiez jamais à des sites douteux
- l'installation de logiciels téléchargés de manière illégale à partir d'internet présente sans aucun doute des risques, étant donné qu'ils pourraient contenir des virus qui pourraient endommager votre ordinateur
- de nos jours, les dispositifs mobiles sont eux aussi la cible de cyber-attaques

Voilà quelques recommandations que les gens d'Eni devraient respecter. Elles sont expliquées en détail dans le règlement de l'entreprise. Voici quelques-unes des recommandations d'Eni.

Quand vous utilisez internet, évitez d'accéder et/ou de visiter des sites web dont le contenu n'est pas en lien avec vos activités professionnelles.

En ce qui concerne les logiciels et les applications, vous devriez éviter d'installer des logiciels non autorisés téléchargés depuis internet ou obtenus à partir d'autres sources sur des ordinateurs ou d'autres dispositifs fournis par Eni.

Et, pour finir, quand vous devez utiliser une SIM de l'entreprise sur votre téléphone personnel, informez toujours le service informatique et faites installer un logiciel de protection supplémentaire.

Pour de plus amples détails, veuillez consulter la procédure « Assigning criteria and utilization rules of ICT resources for individual use ».

5. Médias sociaux et blogs

5.1 Les objectifs de ce module

Les objectifs

Bienvenue dans le cinquième module de ce cours.

Dans ce module, nous analyserons le potentiel et les risques des médias sociaux et nous apprendrons à reconnaître les dangers et à savoir quel comportement adopter vis-à-vis du partage d'informations par l'intermédiaire de ces outils.

Au cours des dernières années, Internet a modifié de manière radicale les modes d'interaction. Les réseaux sociaux et tous les autres éléments du web 2.0 (blogs, forums, wikis, etc.) ont conduit à une explosion de contenus publiés et partagés par les utilisateurs. À moins qu'elles ne soient correctement filtrées et configurées, les informations personnelles et professionnelles peuvent mettre votre sécurité en péril.

5.2 Médias sociaux et web 2.0

Potentiel et risques

Les médias sociaux sont des outils puissants et utiles qui nous permettent de nous connecter avec des amis et des collègues et d'échanger facilement et immédiatement des opinions, des messages et des photos.

Ces dernières années, la croissance rapide de ces outils a changé de manière drastique la façon dont nous partageons les informations. Chaque jour, nous sommes confrontés à des partages, des tweets et des followers. Non seulement nous commentons et publions des contenus mais nous utilisons aussi des contenus publiés par d'autres dans des blogs, des forums et des wikis.

Tout cela présente des risques : le volume croissant d'informations en circulation implique également des personnes potentiellement malintentionnées, qui peuvent utiliser ces outils pour nous attaquer. Par exemple :

- les hackers peuvent utiliser des informations publiques pour sélectionner leur prochaine cible qui sera victime d'un chantage ou pour obtenir des informations sensibles de la part de celle-ci. Ces attaques sont difficiles à reconnaître ;
- les hackers peuvent publier des liens à des sites malveillants ainsi que des virus dissimulés dans des contenus intéressants. Cela incite les personnes à cliquer sur ceux-ci, infectant ainsi leurs ordinateurs.

Précautions

Les médias sociaux ouvrent les portes d'un monde virtuel où il est facile de communiquer et de créer une sensation de confiance. Cependant, dans ce contexte virtuel aussi, il est important de rester sur vos gardes et d'adopter les mêmes précautions que lorsque vous communiquez dans la vie réelle. Pensez-y. Par exemple, dans la vie réelle :

- donneriez-vous vos données, votre adresse, votre numéro de mobile et votre adresse e-mail à un étranger ?
- sélectionnez-vous les amis avec lesquels vous vous confiez et partagez vos pensées ou partagez-vous tout avec qui que ce soit ?
- aimeriez-vous que tout le monde puisse voir une photo embarrassante vous concernant ?
- autoriseriez-vous quelqu'un que vous connaissez à peine à écrire quelque chose sur votre mur ?
- feriez-vous confiance à toutes les informations reçues de la part d'un étranger ?

Posez-vous ces questions quand vous utilisez les réseaux sociaux !

5.3 Le partage d'informations

Profil utilisateur et informations personnelles

Le profil utilisateur est l'un des éléments de base des réseaux sociaux.

Un profil utilisateur est une représentation numérique de l'utilisateur dans un réseau social spécifique.

Souvent, nous ne nous rendons pas compte des risques potentiels liés aux informations publiées pour créer un profil. Prénom, nom, date de naissance, adresse, ville, profession, situation familiale représentent des informations strictement personnelles et peuvent mettre la sécurité de votre ordinateur en péril si elles finissent dans de mauvaises mains.

Quelqu'un pourrait utiliser ces informations pour se faire passer pour l'utilisateur et apparaître crédible. Par exemple, il s'agit des informations typiques requises pour se connecter à des services bancaires mobiles.

Comment pouvez-vous éviter qu'une personne malintentionnée mette la main sur vos informations personnelles ?

En premier lieu, demandez-vous s'il est réellement nécessaire de publier ces informations et soyez vigilant quant aux informations que vous partagez.

Il est également important de configurer vos paramètres de confidentialité de manière à limiter l'accès à ces informations.

Même si vous décidez de ne partager des informations qu'avec vos contacts, vous devez rester prudent vis-à-vis des personnes que vous ajoutez. Faites la différence entre les personnes que vous connaissez réellement et les amitiés virtuelles ; quelqu'un d'autre pourrait se cacher derrière leurs profils.

Informations à propos de votre position et de votre activité

Nous utilisons les réseaux sociaux pour partager des informations à propos de notre vie de tous les jours.

Cela est utile pour rester en contact avec nos amis. Toutefois, il est important de garder à l'esprit que les informations que vous partagez à travers les médias sociaux se répandent immédiatement et, souvent, sans aucun contrôle. En effet, des amis peuvent partager vos informations avec leurs amis et elles pourraient finir dans de mauvaises mains. Bien que vous

essayiez de les retirer, cela pourrait être déjà trop tard. La persistance est l'une des caractéristiques des réseaux sociaux.

Dire à tout le monde où vous vous trouvez et ce que vous êtes en train de faire à tout moment peut être risqué.
Poster des informations depuis votre lieu de travail peut représenter un risque sérieux. Une photo de votre lieu de travail ou de vos collègues pourrait par inadvertance montrer un mot de passe, des documents confidentiels ou d'autres informations cruciales.

Et les choses pourraient même empirer. Des utilisateurs malveillants pourraient associer les informations sur votre profil en ligne et les informations que vous publiez et utiliser cela contre vous.

Informations dissimulées dans des contenus numériques

Partager sans discernement des contenus numériques à travers les médias sociaux peut être extrêmement risqué.

Ce type de contenus peut dissimuler des informations potentiellement dangereuses. Ces informations, appelées métadonnées, décrivent le contexte dans lequel un fichier a été créé. Jetons un œil sur quelques exemples :

- un document peut inclure le nom de l'auteur, l'ordinateur sur lequel il a été créé ou toute autre information relative à l'entreprise
- des photos peuvent contenir des détails dissimulés, les plus cruciaux étant les coordonnées géographiques de l'endroit où la photo a été prise.

Si l'on ajoute ces éléments au partage de nombreuses informations avec des paramètres de confidentialité incorrects, cela peut augmenter les risques potentiels. Par exemple :

- un hacker peut analyser des documents trouvés sur un moteur de recherche, récupérer des informations sur la configuration des postes de travail de l'utilisateur, et appliquer des techniques et des méthodes efficaces pour une attaque
- en analysant les métadonnées d'une photo publiée, les hackers peuvent facilement récupérer des informations sur le lieu où la photo a été prise. Et en croisant ces références avec d'autres informations, ils pourraient même découvrir où vit cette personne.

Il est facile de se protéger :

- soyez toujours vigilant vis-à-vis des contenus numériques que vous partagez
- gérez correctement les paramètres de confidentialité de votre média social.

5.4 Protéger votre entreprise en vous protégeant vous-même

Précautions à adopter

Dans ce module, nous avons souligné combien il est important d'utiliser les médias sociaux avec attention afin d'éviter que vos informations personnelles ne finissent dans de mauvaises mains.

Cela protègera votre entreprise et vous-même contre toute attaque potentielle.

En résumé, voici quelques petits conseils :

- contrôlez soigneusement quelles sont les informations que vous partagez et avec quel type de langage vous les partagez. Cela pourrait être blessant ou constituer un risque si elles étaient utilisées de manière incorrecte
- contrôlez avec qui vous partagez ces informations et gérez vos paramètres de confidentialité de manière à éviter de rendre vos informations publiques en sélectionnant les amis qui peuvent les consulter
- en ce qui concerne les contenus publiés par d'autres, soyez vigilant aux liens et aux documents, qui pourraient dissimuler des pièges
- en particulier, abstenez-vous de poster des photos de votre lieu de travail afin d'éviter de divulguer des détails qui pourraient mettre la sécurité de votre entreprise en péril
- ne postez pas, ne commentez pas, ne tweetez pas au nom ou pour compte d'Eni, à moins que vous n'ayez reçu l'autorisation d'agir en ce sens.

Les médias sociaux sont des moyens de communication de masse, comme la radio, les journaux ou la télévision. Par conséquent, ils font l'objet de règles de communications externes émises par Eni.

Pour de plus amples détails au sujet des règles de communication externe émises par Eni par l'intermédiaire des canaux informatiques, veuillez faire référence aux lignes directrices du système de gestion en matière de communication externe.

Pour de plus amples détails en matière de politiques de protection des marques et de gestion des informations privilégiées au sein d'Eni, veuillez faire référence respectivement aux lignes directrices du système de gestion en matière de gestion de l'identité et d'abus de marché.

6. E-mail et phishing

6.1 Les objectifs de ce module

Les objectifs

Bienvenue dans le sixième module de ce cours.

Dans ce module, nous nous concentrerons sur les attaques par e-mail. Nous soulignerons quelques règles quant à l'utilisation de l'e-mail professionnel, approfondirons la notion de phishing et définirons les mesures de protection à adopter.

6.2 Utiliser l'e-mail professionnel

Partage d'informations par e-mail

L'e-mail est un outil privilégié pour partager des informations sur le lieu de travail. Eni a établi une série de règles et de comportements afin de prévenir des situations qui pourraient compromettre la sécurité de l'entreprise. Jetons un œil sur certains de ceux-ci :

- ne pas utiliser l'e-mail professionnel pour sa correspondance privée ou tout autre but qui ne soit pas en relation avec votre travail ou votre contrat

- ne pas utiliser l'e-mail pour fournir des informations importantes ou confidentielles à propos d'Eni, comme des programmes, des initiatives stratégiques ou des commentaires sans l'autorisation de la part du responsable des données
- ne pas envoyer d'e-mails interdits contenant des informations confidentielles ou critiques ou des informations qui pourraient avoir des effets juridiques ou contractuels pour Eni

Pour de plus amples détails à propos des e-mails, veuillez faire référence à la procédure « Assigning criteria and utilization rules of ICT resources for individual use ». Souvenez-vous que, lors de la diffusion d'informations en dehors de l'entreprise, vous devez respecter les lignes directrices du système de gestion en matière d'abus de marché et de communication externe.

Pour équilibrer les besoins professionnels et privés de ses employés, Eni vous permet d'accéder à votre boîte e-mail personnelle depuis le bureau. Dans ce cas, malgré toutes les contre-mesures de sécurité instaurées par Eni, les risques d'attaques semblables à celles qui peuvent se produire contre votre ordinateur chez vous persistent. Soyez toujours prudent vis-à-vis de tout comportement qui pourrait ouvrir la porte à des cyber-attaques, comme :

- fournir par inadvertance des informations personnelles
- ouvrir ou accéder à des contenus malveillants qui peuvent infecter votre ordinateur.

Les risques de la cyber-sécurité associés à l'e-mail

Eni fournit une série d'instructions afin d'éviter que les e-mails ne soient exposés aux attaques contre les individus et l'entreprise ; cependant, dans certains cas, c'est à l'utilisateur de décider comment gérer les situations qui pourraient compromettre la sécurité. Étant donné la vitesse à laquelle évoluent les codes malicieux et les cyber-attaques, les contre-mesures technologiques de sécurité ne peuvent pas toujours lutter contre tout type d'attaque. Ces attaques doivent être activées par l'utilisateur, en les convainquant habituellement à installer des codes malicieux ou faire quelque chose qui pourrait avoir des effets potentiellement dangereux. Les e-mails de phishing en sont le parfait exemple. Ils peuvent être préparés d'une manière telle que les anti-spams et les filtres anti-phishing ne sont pas en mesure de les intercepter et de les bloquer, et atteignent donc votre compte e-mail.

Dans les pages suivantes, nous fournirons quelques conseils pour vous aider à identifier les escroqueries par phishing et décider quelles précautions adopter quand vous utilisez votre compte e-mail.

6.3 Phishing

Comment fonctionne le phishing de nos jours

Comment fonctionne le phishing de nos jours ?

De nos jours, la plupart des cyber-attaques compte sur la collaboration involontaire des utilisateurs, en leur faisant prendre des risques. L'e-mail est l'outil principal utilisé pour « capturer » les utilisateurs et les porter à faire ces choses-là.

Les attaques e-mail peuvent vous inciter à agir de différentes manières, comme :

- cliquer sur des liens vers des sites malveillants ou compromis
- ouvrir des pièces jointes malveillantes

- fournir des informations d'accès (ou des informations qui pourraient être utilisées pour des attaques successives), directement ou en visitant des sites et en remplissant des formulaires.

Spear phishing

Le spear phishing est une nouvelle forme de phishing qui se répand rapidement. Il consiste en des e-mails personnalisés avec une référence spécifique à des amis, des intérêts, des activités, de récents échanges d'informations.

Les hackers recueillent des informations en ligne (par exemple, par l'intermédiaire des profils des médias sociaux et en traçant le comportement de navigation) pour créer un profil.

Ces e-mails n'ont pas besoin de rentrer trop dans les détails. Une simple référence au lieu de travail du destinataire peut être très efficace.

Comment reconnaître les escroqueries par phishing

Certains indices vous permettront de reconnaître une escroquerie par phishing.

Dans cet exemple, un utilisateur BccCard reçoit un e-mail qui l'informe qu'il peut télécharger son relevé de compte en cliquant sur un lien.

Mardi 25/11/2014 10:02

BccCard <info831700@cosmont.com>
Relevé de compte nº 982634715

À james.smith@gmail.com

Cher client,

cet e-mail vise à vous informer que votre dernier relevé de compte est maintenant en ligne
Vous pouvez le consulter, l'imprimmer et le sauvegarder sur votre ordinateur.

Veuillez vous rappeler que chaque relevé de compte restera disponible en ligne pendant 3 mois à partir de la date d'émission.

Consultez l'espace client

Nous vous remercions d'avoir choisi les services en ligne de BccCard.
Cordialement.

Vous pouvez remarquer immédiatement que le message est très générique. Il ne définit pas le service et seuls quelques éléments d'interaction sont présents (par exemple les numéros gratuits).

Cependant, d'autres éléments qui devraient vous alarmer qu'il s'agit d'un cas de phishing sont aussi présents.

Fautes d'orthographe

- Fautes d'orthographe évidentes

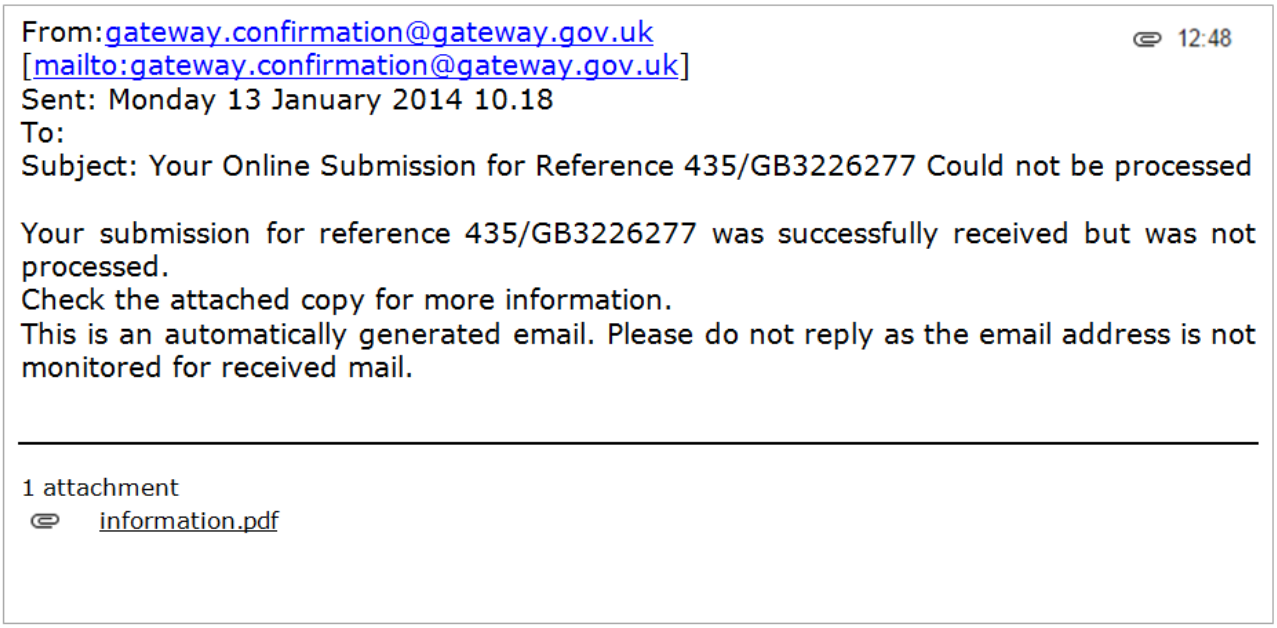
Le nom du lien est générique. De plus, pourquoi la banque devrait ajouter un lien au lieu de vous dire tout simplement d'accéder à votre service en ligne ?

Les risques d'une interaction imprudente avec un e-mail de phishing

Dans le passé, même un clic imprudent pouvait être réversible. Aujourd'hui, ces actions sont irréversibles dès la première seconde. Voici quelques exemples :

- cliquer sur des liens vers des sites malveillants qui infectent clairement votre ordinateur
- installer des logiciels antivirus trompeurs
- ouvrir des fichiers joints HTML (qui possèdent les mêmes effets que les liens malveillants)
- ouvrir des fichiers joints (Word, Excel, PDF, etc.) personnalisés pour apparaître anodins mais qui endommageront votre ordinateur.

Il s'agit d'un exemple d'un e-mail indiqué comme spam car il contient un virus dans le fichier joint.


From:gateway.confirmation@gateway.gov.uk 12:48
[mailto:gateway.confirmation@gateway.gov.uk]
Sent: Monday 13 January 2014 10.18
To:
Subject: Your Online Submission for Reference 435/GB3226277 Could not be processed

Your submission for reference 435/GB3226277 was successfully received but was not processed.
Check the attached copy for more information.
This is an automatically generated email. Please do not reply as the email address is not monitored for received mail.

1 attachment
information.pdf

Dans d'autres cas, vous pouvez encore vous arrêter à temps et changer d'avis. Par exemple :

- quand vous recevez de faux fax ou d'autres documents, qui sont en fait des fichiers exécutables qui exécutent des opérations spécifiques quand ils sont lancés. Au lieu du document que vous attendiez, vous trouverez un message que vous pouvez ignorer.
- quand vous accédez à des sites qui demandent les données d'identification pour y avoir accès de manière frauduleuse ou pour vous inciter à télécharger ou mettre à jour un logiciel ou des plugins. Le simple accès à ce site ne compromettra pas votre ordinateur, donc vous avez encore le temps de vous arrêter.

6.4 Protéger votre entreprise en vous protégeant vous-même

Précautions à adopter

Récapitulons ce que nous avons appris dans ce module.

En ce qui concerne l'utilisation de votre e-mail professionnel :

- il existe des règles précises en ce qui concerne l'utilisation de votre e-mail professionnel
- vous pouvez accéder à votre boîte e-mail personnelle depuis le bureau.

Que vous soyez chez vous ou au bureau, soyez vigilant à ce que vous dites et vis-à-vis des personnes avec lesquelles vous communiquez pour éviter de divulguer des informations personnelles et d'ouvrir les portes aux cyber-attaques.

En ce qui concerne les risques de phishing :

- l'e-mail est un moyen rapide de réaliser un grand nombre d'attaques. Soyez extrêmement vigilant lorsque vous utilisez cet outil
- des e-mails extrêmement détaillés peuvent également être des escroqueries, à cause de la facilité avec laquelle les informations personnelles peuvent être récupérées sur internet. Soyez particulièrement prudent en cas de messages génériques qui font référence à des groupes auxquels vous appartenez, à votre entreprise et à toute autre information utile
- les e-mails de phishing contiennent des indices que vous pouvez trouver
- une anomalie après une interaction avec un e-mail de phishing peut signifier que votre ordinateur est compromis.

7. Les nouvelles frontières des attaques par ingénierie sociale

7.1 Les objectifs de ce module

Les objectifs

Bienvenue dans le septième et dernier module de ce cours.

Dans ce module, nous analyserons quelques informations concernant les attaques contre le secteur de l'énergie et nous apprendrons à connaître un certain nombre de nouveaux scénarios d'attaque outre ceux les plus fréquents que nous avons analysés jusqu'à maintenant.

Les scénarios d'attaques par ingénierie sociale évoluent constamment. L'évolution rapide des technologies et des comportements sociaux fournit aux hackers de nouvelles opportunités de menaces contre la sécurité informatique.

7.2 Les attaques contre le secteur de l'énergie

La nature des attaques ciblées

Les cyber-attaques sont devenues fréquentes, et ont toujours un objectif clair :

- l'idéologie, dans le cas du « hacktivisme »
- l'information, dans le cas de l'espionnage industriel
- l'argent, dans le cas des cyber-crimes.

C'est pourquoi les attaques ciblées augmentent, outre celles plus génériques.

Des tendances récentes montrent comment le secteur de l'énergie est en train de devenir l'une des cibles les plus fréquentes d'attaques, notamment les attaques par ingénierie sociale. Les hackers attaquent les utilisateurs qui, par inadvertance, sont le maillon le plus faible de la chaîne de sécurité informatique d'une entreprise

Ce à quoi ressemble une attaque contre le secteur de l'énergie

Une analyse des dernières attaques contre les plus importantes sociétés au monde publiée par Fortune 500 révèle de nombreux exemples d'attaques ciblées. Un exemple récent est la cyber-attaque contre Statoil, l'un des groupes pétroliers les plus importants au niveau européen.

43	Aug 20	?	UPS	UPS admits that 51 of its franchised stores were hit with a malware attack that put customer credit and debit card data at risk from Jan. 20 to August 11.	POS Malware	Courier	CC	US	182 50
44	Aug 27		JPMorgan Chase & Co.	Bloomberg news reveals that hackers allegedly from Russia targeted JPMorgan Chase & Co. (JPM) and at least four other banks in a coordinated attack on major financial institutions. One month later the real entity of the attack will be revealed: **76 million** households.	Targeted Attack	Finance	CC	US	57 18
45	Aug 27	?	Statoil	50 Norwegian oil and energy companies have been hacked, and 250 more have been warned to check their networks and systems for evidence of a breach. Among the likely targets is Statoil, Norway's largest oil company.	Targeted Attack	Oil	CE	NO	54
46	Sep 2	?	The Home Depot	The Home Depot confirms that hackers compromised the payment systems in its **2,200** stores in the US and Canada and stole credit and debit card data. The Home Depot believes that **56 million** credit cards have been compromised by criminals.	POS Malware (Backoff)	Retail	CC	US	102 33
47	Sep 29	?	SUPERVALU	Supervalu announces that a new malware is discovered in late August or early September 2014 for some of its Shop 'n Save, Shoppers Food & Pharmacy and Cub Foods stores. The new breach appears to have no connection to the one announced in mid-August 2014	POS Malware	Retail	CC	US	94

L'article décrit une attaque, qui, selon l'enquête, était une attaque de spear phishing lancée de manière ordinaire :

- un e-mail a été envoyé à un groupe de personnes clés de l'entreprise
- l'e-mail semblait provenir de personnes bénéficiant de positions clés au sein de l'entreprise
- il contenait un fichier joint malveillant qui, une fois ouvert, permettait au hacker de prendre le contrôle de la machine.

Des nouveautés comme celles-ci soulignent comment les attaques par ingénierie sociale sont des faits réels et combien il est important de sensibiliser les personnes aux règles de comportement pour se protéger soi-même ainsi que l'entreprise.

Pendant ce cours, nous avons examiné quelques scénarios. Toutefois, il est important d'être préparé à de nouveaux scénarios et aux nouvelles méthodes utilisées pour menacer la sécurité informatique. Et c'est ce sur quoi nous allons maintenant nous concentrer.

7.3 Les nouveaux scénarios d'attaque

Les nouveaux canaux de phishing

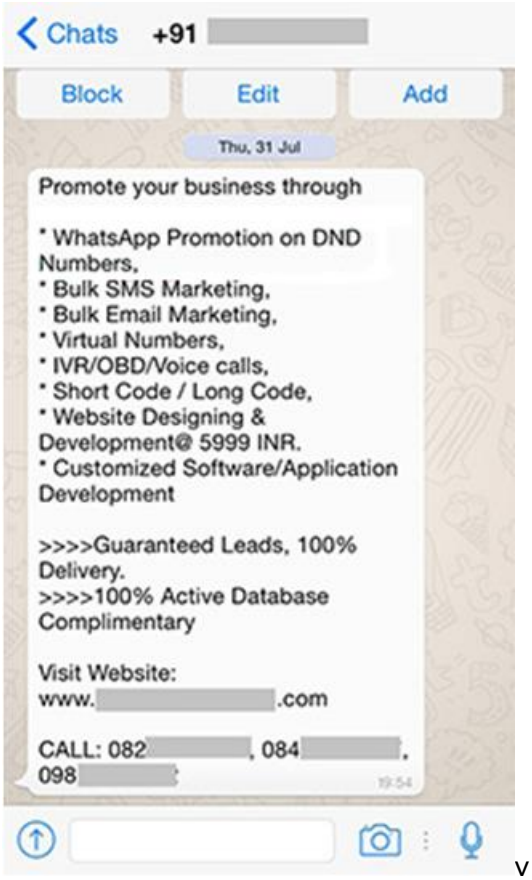
De nouvelles tendances montrent dans quelle mesure les autres canaux, comme les SMS, les médias sociaux et les autres systèmes de messagerie instantanée sont utilisés, en plus des e-mails, pour tromper les utilisateurs.

D'un point de vue psychologique, un SMS en provenance d'un ami ou un message sur Facebook ou Whatsapp possèdent une crédibilité plus importante. Une attaque lancée par l'intermédiaire de ces canaux de communication peut être plus efficace.

SMSishing est en train de devenir un mot très populaire pour décrire des attaques contre les applications de messagerie mobile.

Ces escroqueries sont en train de devenir de plus en plus réalistes, étant donné les nombreuses modalités de compromettre un dispositif mobile ou un compte Facebook.

Jetez un œil sur cet exemple d'escroquerie Whatsapp.



v

Comme vous pouvez le voir, le message contient de nombreuses erreurs ainsi que des liens douteux, ce qui fait que cette escroquerie par phishing est facile à identifier. Ces escroqueries peuvent aujourd'hui sembler simplistes, mais dans un futur proche, elles deviendront certainement plus sophistiquées et efficaces, suivant la même évolution que les attaques par e-mail.

Ainsi, gardez toujours à l'esprit que :

- les e-mails ne sont pas les seuls moyens disponibles pour les escroqueries par phishing
- soyez toujours extrêmement vigilant avant de cliquer sur un lien reçu par l'intermédiaire d'une messagerie instantanée.

Les plateformes sécurisées : un faux mythe

La technologie réduit les distances, et nous travaillons souvent hors du bureau. Nous sommes habitués à accéder à nos e-mails ou à d'autres services de l'entreprise depuis notre mobile ou modifier des documents sur notre ordinateur.

Pour nous protéger contre les cyber-attaques, nous comptons souvent sur ce que l'on considère comme des technologies et des plateformes intrinsèquement fiables. Cependant, les cyber-menaces répondent souvent à des fins commerciales. Les hackers attaquent la « masse » pour augmenter leurs chances de succès.

Par exemple, le fait qu'Android soit la plateforme la plus attaquée peut être expliqué par sa popularité et ses caractéristiques, qui permettent de rendre certaines escroqueries plus faciles.

Sur le long terme, des déclarations comme « j'ai un antivirus, de toute façon », ou « j'ai un iPhone, qui est plus fiable, de toute façon » s'avèrent être de faux mythes.

De plus, c'est un fait que les antivirus ne reconnaissent que des codes malicieux connus et ne sont pas efficaces en cas de nouveaux types d'attaques, notamment si elles sont lancées par l'intermédiaire des comportements des utilisateurs.

Donc, soyez vigilant :

- il ne suffit pas de dire « mon système est fiable » et de compter sur la seule technologie pour se protéger contre les cyber-attaques, car la situation est en constante évolution.
- il est crucial d'être conscient de vos actions et d'adopter un comportement prudent.

Qu'en est-il du futur ?

De nos jours, la technologie est omniprésente. De nombreux objets intelligents se présentent à nous : télévisions, réfrigérateurs, voitures, verres et même des feux tricolores, consoles de jeux vidéo et thermostats connectés au web pour nous permettre de transmettre et de télécharger des informations. Cela s'appelle l'Internet des objets, et est en train de devenir de plus en plus important.

D'un côté, la popularité de cette technologie rend nos vies plus faciles. De l'autre, elle introduit des menaces possibles à la sécurité informatique. Ces dispositifs ne sont pas toujours assez mûrs de ce point de vue ; par conséquent, les hackers peuvent les compromettre facilement.

L'idée qu'une télévision ou un réfrigérateur puisse faire l'objet d'une attaque peut sembler absurde, mais, malheureusement, ce type d'agression représente déjà une réalité.

Et ce n'est que le début. Ces dispositifs intelligents peuvent devenir l'un des moyens utilisés pour lancer de nouvelles attaques. À bien des égards, ils le sont déjà ! Il suffit de penser aux récentes attaques contre les routeurs à domicile. Nous considérons souvent ces dispositifs comme de simples « boîtes », mais il s'agit en réalité de véritables ordinateurs comprenant différents modes d'interaction, qui peuvent être activés pour contrôler l'accès et la sécurité de millions de réseaux domestiques.

7.4 Conclusions

Conclusions

Dans ce dernier module, nous avons appris que les attaques par ingénierie sociale sont des faits, et non pas de la fiction. Par conséquent, la sensibilisation aux risques dissimulés derrière l'utilisation de la technologie peut aider à mettre en place de bonnes pratiques.

Nous avons aussi vu que les scénarios d'attaque ne cessent d'évoluer rapidement. Dans un futur proche, ils pourraient aussi se diffuser aux objets les plus inattendus. C'est pourquoi la sensibilisation à ces risques aujourd'hui peut aider à lutter contre les cyber-menaces de demain.

Si vous désirez en savoir plus sur les thèmes abordés dans ce cours ou envoyer un signalement ou une suggestion, envoyez-nous un message à l'adresse e-mail sicurionline@eni.com