Gendarmerie nationale

Région de gendarmerie Nouvelle-Aquitaine
Antenne Sécurité Économique et Protection des Entreprises de la formation administrative de Poitou-Charentes
Groupement de gendarmerie départementale de la Vienne.

Alerte

ESCROQUERIE PAR FAUX PRESTATAIRE D'EDF

Un individu se présentant comme salarié du bureau d'études d'EDF entreprises contacte une société pour réaliser un bilan complet gratuit de sa consommation électrique en vue de lui faire réaliser de substantielles économies.
II propose rapidement une solution miracle permettant un gain de 20 %, passant par l'installation de batteries de condensateurs pour réguler les pics de consommation.
A l'issue de l'entretien téléphonique, le dirigeant reçoit par mail deux documents visant à finaliser les différentes propositions, auxquelles aucune suite ne sera heureusement donnée.
En effet, après vérifications faites directement auprès des services d'EDF, il s'avère que les documents transmis sont des faux grossiers et que les tarifs du matériel proposé sont largement supérieurs à ceux du marché.

QUE FAIRE ?

Si vous êtes confronté à pareille situation, voici quelques conseils simples à appliquer :

- Si l'interlocuteur semble suspect, dès le début des échanges, lui demander de vous donner votre numéro client et/ou le montant de votre dernière facture.
- Ne pas répondre à ce type de sollicitation et surtout ne communiquer aucune information.
- Contacter rapidement votre conseiller « EDF Entreprises ». Si l'usage frauduleux de la marque EDF entreprises est prouvé, EDF engagera immédiatement des poursuites.
- Transférer les messages douteux à l'adresse suivante : message-frauduleux@edf.fr
- Déposer plainte auprès du commissariat ou de la gendarmerie. L'usurpation d'identité, même la simple tentative est un délit. Vous munir de tout document pouvant aider à identifier l'auteur (nom de l'entreprise et de l'interlocuteur, adresse, numéro de téléphone, objet du démarchage, copie des e-mails et des pièces jointes, etc.

L'été est une période propice aux fraudes et attaques en tous genres.
Escroquerie au faux président ou à la fausse domiciliation bancaire, ransomware, phishing, démarchage téléphonique, piratage de serveur téléphonique….
Les escrocs et pirates informatiques en tous genres ne manquent pas d'imagination pour s'en prendre à vos actifs financiers.
Il convient donc de faire preuve d'une vigilance de tous les instants.
Ne pas déposer plainte, permet aux escrocs de poursuivre leurs activités délictuelles en toute impunité.

AU MOINDRE DOUTE, ALERTEZ IMMÉDIATEMENT LES FORCES DE L'ORDRE

Gendarmerie nationale

Région de gendarmerie Nouvelle-Aquitaine
Antenne Sécurité Économique et Protection des Entreprises de la formation administrative de Poitou-Charentes
Groupement de gendarmerie départementale de la Vienne.

VIGILANCE CARTE BLEUE

Carte Bancaire (CB) : Moyen de paiement le plus usité lors des transactions financières par les particuliers et certaines PME.

DE QUOI PARLE T-ON ?

Le paiement par carte bancaire souvent appelée carte bleue (CB) est devenu "monnaie courante" dans notre monde actuel.
Le volume des transactions effectuées quotidiennement est gigantesque.
La tentation est donc grande pour bon nombre d'escrocs de voler la carte bleue ou les données qu'elle contient, par tous les moyens « physiques ou numériques ».
Une meilleure connaissance des risques liés aux facilités de vol des informations contenues dans une carte bancaire doit permettre à son détenteur de mieux se prémunir.

Explications :

Si le vol physique de ces cartes représentait encore il y a peu le plus grand risque, désormais les nouvelles technologies rendent possible d'autres types d'exactions notamment le piratage numérique.
- Le vol des informations et du code de la carte réalisé par des escrocs peut se faire sur un Distributeur Automatique de Billets (DAB) en insérant un dispositif électronique permettant, dans un premier temps, de visualiser le code de sécurité de la carte saisi par son propriétaire et, dans un second temps, de récupérer la CB provisoirement bloquée dans le distributeur.
- Le paiement sans contact se démocratisant ces dernières années rend les paiements encore plus rapides mais aussi plus vulnérables :
Depuis quelques mois, un moyen simple d'utilisation permet de pirater les CB. L'escroc se dote d'une application qui scanne à courte distance (50 cm à 1 m) tous les appareils équipés de la technologie NFC (utilisée lors des paiements sans contact) pour subtiliser les informations bancaires.
- Paiement sur Internet. Une fois les données validées, elles sont transmises sans retour possible.
- Phishing message contenant un programme malveillant qui s'installe sur votre ordinateur et récupère vos données et informations bancaires. Message intrusif réclamant vos identifiants (login – mot de passe) et vous dirige vers un faux site bancaire.

Précautions :

- Sur votre ordinateur, ne pas cliquer sur des pièces jointes dont vous ne connaissez pas la provenance.
- Dotez-vous d'un antivirus incluant une protection bancaire.
- Ne donnez jamais vos identifiants bancaires. Aucune banque ne réclame ces informations par courriel !
- Effectuez vos achats sur Internet à l'aide d'une @carte (carte virtuelle éphémère attribuée par votre banque valable pour un seul type d'achat, pour un seul montant et pour un jour précis).
- Ne payez que sur des sites sécurisés dont l'adresse commence par https.
- Protégez-vous des regards indiscrets lorsque vous payez à un guichet, à une caisse ou si vous retirez de l'argent à un distributeur automatique.
- Sachez qu'un commerçant doit obtenir votre approbation pour utiliser le paiement sans contact de votre CB.
- Protégez votre CB équipée du paiement sans contact au moyen d'étuis empêchant l'interception frauduleuse des signaux émis de votre CB ou, si vous le souhaitez, demandez à votre banque de désactiver la technologie NFC.
- Consultez régulièrement les relevés de votre compte bancaire pour signaler toute anomalie à votre banque.

Réactions :

Dès que vous êtes victime ou que vous pensez l'être, réagissez de la façon suivante :
- Vérifiez auprès de votre banque si des transactions illicites ont été passées sans votre accord.
- Une plainte doit être déposée auprès des forces de l'ordre (Police/Gendarmerie) en cas de vol de carte bleue, de vol d'informations ou de données.

AU MOINDRE DOUTE, ALERTEZ IMMÉDIATEMENT LES FORCES DE L'ORDRE