Panoptinet

Gardez un oeil sur votre réseau

Phishing : EDF rembourse !

admin · Monday, September 12th, 2011

Les bonnes nouvelles peuvent en réalité cacher une bien mauvaise surprise. C'est le cas de cette arnaque du web (phishing), où, sous le couvert d'un mail EDF promettant un remboursement, un cyber-escroc cherche à vider votre compte bancaire. Prudence !

En fin de semaine dernière, deux internautes averties ont alerté Panoptinet sur une **nouvelle tentative de phishing**, reprenant cette fois **les traits d'EDF**. Plus aboutie que la dernière tentative (Des clients EDF victimes d'arnaque en ligne), cette nouvelle campagne d'hameçonnage est aussi **plus incitative** (promesse de remboursement). Le piège reste cependant détectable, pour peu que l'on prête un peu d'**attention au mail de départ** :

Date: Fri, 9 Sep 2011 12:05:54 +0200
To: [redacted]@live.fr
Subject: Erreur de prélèvement (Rappel)
From: support@edf.fr

Bienvenue chéz EDF - France

Cher membre EDF,
Apres plusieurs tentative inutile de vous joindre par telephone,nous vous avons envoye ce mail pour vous informer qu une defaillance est survenue lors des prelevements mensuels effectues sur le compte de notre clientele ,en effet le 03 avril 2011 votre compte a ete indument debite de la somme de (32.30) Euro. Cette confusion est essentiellement du la correspondance de vos noms et prenoms avec ceux d un autre client . A fin de proceder a un de remboursement immediat nous vous prions de bien vouloir cliquer sur le lien ci-dessous et fournir toute information susceptible d accelerer ce remboursement .
Remplissez le formulaire de remboursement en cliquant sur le le lien suivant :
Veuillez Cliquer ici :
Important :
Le versement effectue par EDF sera porte sur votre prochain releve bancaire. Nos clients EDF beneficieront d un geste commercial. Nous vous assurons de la confidentialite des informations fournies EDF se porte garant quant la responsabilite juridique de ces transactions. Nous vous remercions de votre comprehension et nous nous excusons pour le desagrement encouru.

Sincères salutations,
L'équipe EDF

Nous Contacter

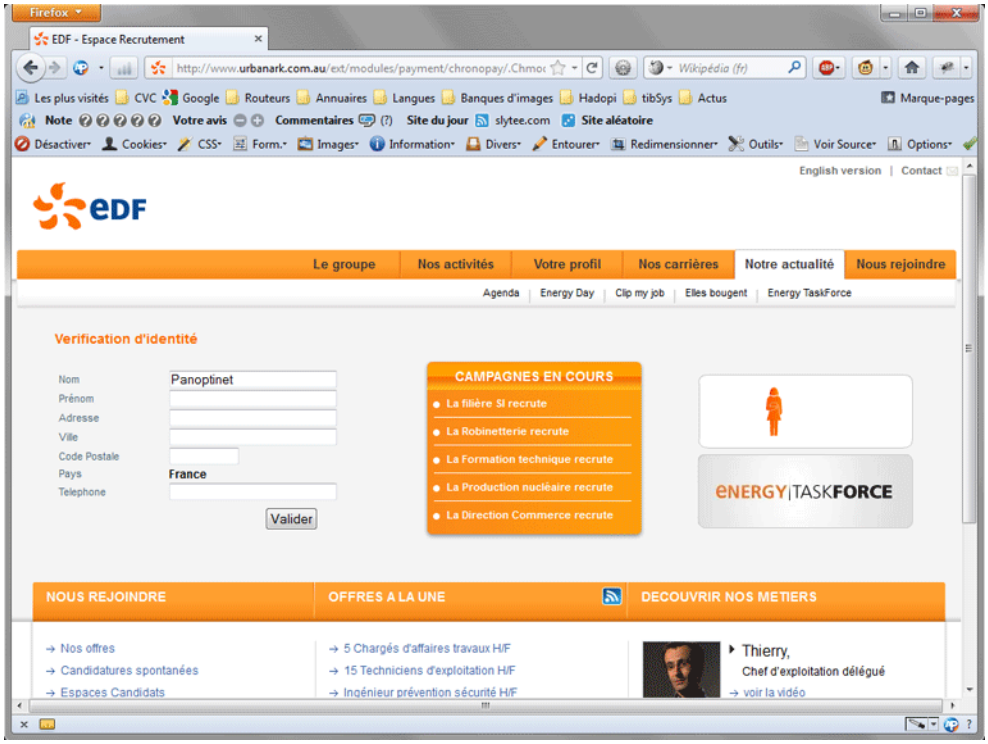
Par téléphone au 3244 *
Par Fax: +33 899 90 5000 (1,35€ par appel puis 0,34€/mn)
Par courrier: EDF Haut Débit - 75371 Paris Cedex

EDF est certifié NF Service pour la qualité de sa relation client.

Informations légales relatives au forfait EDF
* gratuité du temps d'attente à partir d'une EDF, tarif local puis prestation d'assistance à 0,34€/mn sur facture EDF

Si **l'adresse de l'expéditeur paraît officielle**, et que tous **les éléments nécessaires sont présents** (logos EDF et NF, contact, promesse de confidentialité, etc.), l'œil averti remarquera tout de suite les **nombreuses fautes d'orthographe**, les tournures de phrases alambiquées et le manque de ponctuation. **Peu crédible** pour un mail censé provenir du premier fournisseur d'électricité en France ! A noter aussi qu'à aucun moment le numéro de client n'est mentionné...

Le cyber-escroc à l'origine de ce **mail frauduleux**, sur la masse de messages envoyés, espère cependant que quelques destinataires se feront avoir. Et c'est systématiquement le cas ! Pour peu que le lecteur parcoure un peu rapidement le texte, ou qu'il ne prête pas attention aux incohérences, celui-ci **clique sur le lien proposé** en vue d'obtenir le **remboursement (32,30 €)** promis dans le mail. C'est là que le piège commence à se refermer :



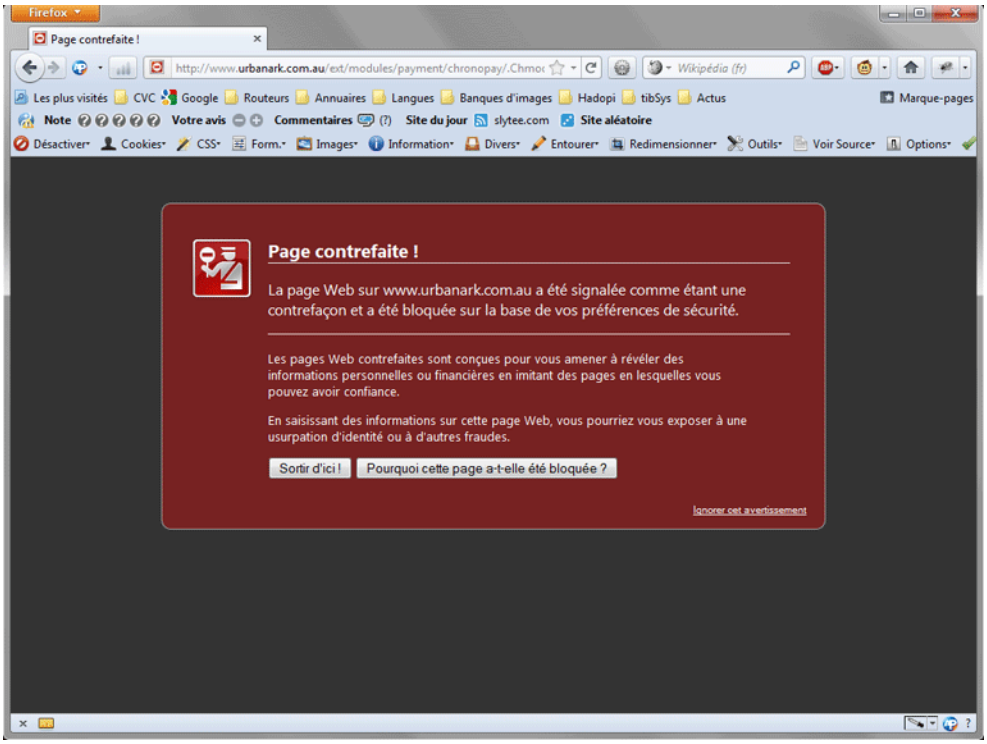
Le site de destination ressemble trait pour trait au site officiel d'EDF, mais ce n'est qu'une **copie**. Tous les liens fonctionnent et renvoient même vers le site officiel. Mais regardez bien l'**adresse URL** de la page : il ne s'agit pas de france.edf.com ni de bleuciel.edf.com, mais de **urbanark.com.au**. C'est maintenant certain, il s'agit d'un **site falsifié**, probablement frauduleux. En effet la page proposée demande directement de fournir des premières **informations personnelles** : nom, prénom, adresse, téléphone. Ne le faites surtout pas ! Vos informations personnelles sont précieuses.

Après validation, la **"vérification d'identité"** se poursuit avec la demande de vos **identifiants bancaires** : nom de la banque, numéro de la carte, nom du détenteur, numéro de compte, etc.

Le piège se referme définitivement ici. Ces identifiants bancaires sont ensuite utilisés directement par le cyber-escroc, ou revendus sur les supermarchés virtuels de cartes bleues volées.

Une fois que l'internaute piégé valide ces informations, il est ensuite redirigé vers la page d'accueil du site d'EDF, la vraie cette fois, sans autre forme de politesse : le mal est fait.

Heureusement, cette **tentative d'hameçonnage** a vite été détectée et rapportée auprès des **navigateurs internet**, qui sont les seuls capables d'avertir à temps les internautes crédules. **Firefox** a ce week end mis en place une **alerte** (voir image ci-dessous), et **Panoptinet a averti les services Microsoft** pour le navigateur Internet Explorer. **Chrome**, le navigateur par Google, indique lui aussi la possibilité d'une tentative de phishing lorsque l'on arrive sur la page incriminée.



Prudence donc lorsque vous consultez vos mails, on ne le répètera jamais assez !

Merci à Emilie G. et Rachel A. pour nous avoir alertés, et transmis le mail frauduleux !

Image : By user:AnonMoos (Own work) [Public domain], via Wikimedia Commons

This entry was posted on Monday, September 12th, 2011 at 4:26 pm and is filed under Actualités décryptées par Panoptinet
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.