

Commentaires sur le message frauduleux

du 8 octobre 2017

« Messagerie Outlook : dernier rappel avant migration le 30 octobre »

La messagerie d’un ancien étudiant a été piratée, et la ou le pirate a pu y trouver des informations telles que :

* l ’Université de Poitiers a effectué une migration vers la messagerie Zimbra (en 2015) ;
* l’Université de Poitiers propose Office 365 (avec la messagerie Outlook) aux étudiants et personnels pour un usage personnel, depuis le printemps 2017.

La ou le pirate s’est, par ailleurs, appuyé(e) sur des informations provenant d’autres universités françaises ayant aussi effectué une migration de messagerie (université Paris Dauphine en l’occurrence), pour construire son message qui peut paraître crédible au premier abord.

Cependant, une lecture plus attentive montre vite des incohérences. Seules les formulations

douteuses sont commentées. Elles portent sur le contexte, les formulations techniques étant, elles, relativement crédibles.

De: "Communication interne" <jean.@etu.univ-poitiers.fr>

Envoyé: Dimanche 8 Octobre 2017 15:41:59
**Objet:** Messagerie Outlook : dernier rappel avant migration le 30 octobre

Bonjour,

Comme vous le savez sûrement suite aux différentes communications faites depuis le 08 october, Université de Poitiers va migrer sa messagerie de Zimbra vers Office 365 lundi 30 octobre. Cette migration sera effective pour tous les domaines de messagerie en @etu.univ-poitiers.fr ou apparentés comme @univ-poitiers.fr.

Cette opération va mobiliser tout le centre de support et toute la DSI et ses prestataires afin que les opérations se déroulent le plus facilement possible pour l'ensemble des utilisateurs. La migration technique a déjà démarré et est en cours, mais il est important que vous preniez connaissance des informations recensées dans la page web suivante :

CLIQUEZ ICI POUR ACCEDER SUR LA MIGRATION MESSAGERIE VERS OFFICE 365.

Merci de vous y rendre impérativement dès que possible afin d'avoir toutes les informations utiles, de connaître précisément le déroulement des opérations, la vitesse à laquelle vos anciens emails arriveront dans votre nouvelle boîte aux lettres et les limites de la migration, c'est à dire les différents éléments qui ne pourront pas être migrés (les tags par exemple) et pour lesquels vous devez bloquer un peu de temps pour les reproduire dans le nouvel environnement.

Cette page est susceptible d'être mise à jour en fonction de l'évolution de la migration, n'hésitez pas à revenir la consulter régulièrement d'ici le 30 octobre.

Toute l'équipe est mobilisée en permanence et reste à votre disposition quelles que soient vos questions.

Bien cordialement

Sébastien Fournier et Miguel Membrado

Pôle Numérique

Direction des Systèmes d'Information

+33630751933

CONCLUSIONS

Les personnes qui ont fourni leurs identifiant et mot de passe de compte Sel en réponse à ce message en ont subi de nombreux désagréments.

Si elles utilisaient ces paramètres d’authentification pour d’autres comptes que le compte Sel (messagerie personnelle, compte d’achats en ligne…), bien que cela soit plus que déconseillé, les conséquences sont encore plus dommageables.

En conclusion de cette arnaque, et pour anticiper sur celles à venir, il faut retenir de :

* n’utiliser les identifiant et mot de passe de compte Sel **que pour le compte Sel** ;
* vérifier systématiquement dans la barre d’adresse du navigateur web l’adresse de la page web vers laquelle renvoie le lien contenu dans un message électronique ;
* s’assurer de la crédibilité des émetteurs du message (existence dans l’annuaire de l’UP, statut adéquat).

Des INFO Déj’ (rencontres d’une heure en début de journée pour échanger sur un thème informatique) vont être systématisés à partir de novembre 2017, de façon à ce que chacun puisse mieux comprendre le cadre existant, et savoir comment contribuer, à son niveau, à la sécurité informatique de l’établissement.