Bonnes pratiques

Lorsque vous recevez un message provenant a priori d'un établissement bancaire ou d'un site de commerce électronique il est nécessaire de vous poser les questions suivantes : Ai-je communiqué à cet établissement mon adresse de messagerie ? Le courrier reçu possède-t-il des éléments personnalisés permettant d'identifier sa véracité (numéro de client, nom de l'agence, etc.) ?

1. Connectez-vous toujours en tapant l'adresse de votre organisme bancaire dans votre navigateur (https://ebanking.cdm.co.ma) ;
2. Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par https et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur, et que le domaine du site dans l'adresse correspond bien à celui annoncé (gare à l'orthographe du domaine) !
3. Ne passez jamais par un moteur de recherche comme Google pour localiser votre banque car les hackers peuvent parfois faire apparaître leur faux site dans les résultats de Google ;
4. Même si l'adresse comprise dans l'email est conforme à l'adresse officielle de votre banque, il reste très facile pour le pirate de vous renvoyer vers un site frauduleux. Vérifiez toujours que le site sur lequel vous êtes connecté correspond bien exactement, à la lettre près, au site de votre banque ;
5. Ne jamais cliquer sur un lien compris dans un email où l'on demande au destinataire de se connecter afin de réactiver un compte bancaire ou de réaliser des modifications sur ce compte ;
6. Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet rare (voire impossible) que le Crédit du Maroc vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone !
7. Signaler immédiatement à votre agence, tout email suspect, même si vous n'avez pas la certitude qu'il s'agit d'un mail de phishing ;
8. Pour protéger vos postes de travail contre le piratage, il est vivement recommandé d’appliquer les mesures préventives suivantes :
    - Vérifier l’état de vos postes de travail (Version OS légal, antivirus à jour) ;
    - Vérifier l’absence d'un Keylogger matériel (Enregistreur de touches du clavier) au niveau de vos postes de travail ;
9. Afin de se protéger contre les spams infectieux (mail porteur de pièce jointe infectieuse), il est recommandé de :
    - Ne pas ouvrir le mail ni la pièce ;
    - Détruire le mail ;
    - Si la pièce a été ouverte, un Scan antivirus complet sur le PC doit être réalisé, puis changer l'ensemble des mots de passe ;
10. Pour protéger vos Smartphones contre le piratage, il est vivement recommandé d’appliquer les mesures préventives suivantes :
    - Ne pas installer des applications des éditeurs anonymes sur vos Smartphone ;
    - Installer un Antivirus à jour sur vos Smartphones ;
    - Signaler immédiatement, tout Email ou SMS suspect demandant le téléchargement d’application ;
    - Protéger vos téléphones par un mot de passe ;
    - Contacter votre agence en cas d'indisponibilité de vos numéros de téléphone ;