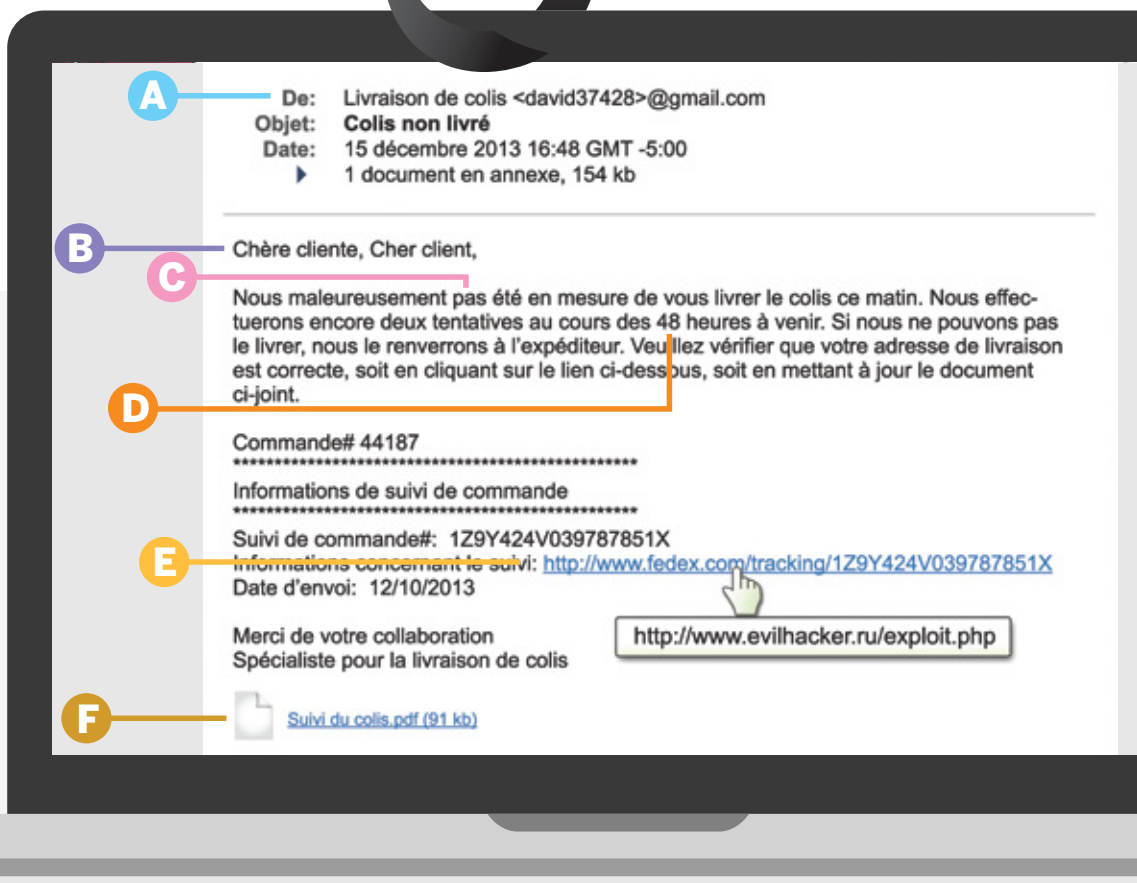
Ne vous faites pas HAMEÇONNER

La Capitale

Que ce soit à votre adresse de courriel professionnel ou à votre adresse de courriel personnel (gmail.com, hotmail.com, etc), vous avez probablement déjà reçu des messages de type hameçonnage. *Si vous cliquez sur les liens présents dans ces messages ou si vous ouvrez les pièces jointes, vous pourriez avoir de sérieuses surprises, vraiment pas agréables.* Évitez de mordre à l'hameçon que vous tendent les fraudeurs en repérant les indices.



A Vérifiez les **ADRESSES COURRIEL.** Si le courriel semble venir d'une organisation légitime, mais que l'adresse « de » est celle d'un compte personnel, comme @gmail.com ou @hotmail.com, il s'agit certainement d'une attaque. Pensez aussi à vérifier les champs « À » et « Cc ». Le courriel est-il envoyé à des gens que vous ne connaissez pas ou avec qui vous ne travaillez pas ?

B Méfiez-vous des courriels commençant par « Chère cliente, Cher client » ou toute autre forme de **SALUTATION GÉNÉRIQUE.** S'il s'agit d'une organisation digne de confiance qui a besoin de vous contacter, ils devraient connaître votre nom ainsi que d'autres informations vous concernant. Pensez aussi à vous demander si vous attendez un courriel de cette entreprise.

C Faites preuve de méfiance si le message contient des **FAUTES DE GRAMMAIRE OU D'ORTHOGRAPHE.** La plupart des entreprises relisent soigneusement leurs messages avant de les envoyer.

D Méfiez-vous de tout courriel qui demande une **« ACTION IMMÉDIATE »** ou qui crée un sentiment d'urgence. Il s'agit d'une technique courante pour pousser les gens à commettre des erreurs. Rappelez-vous que des organisations légitimes ne vous demandent pas vos informations personnelles.

E **SOYEZ PRUDENT AVEC LES LIENS,** et ne cliquez que sur ceux que vous attendez. Glissez aussi votre souris sur le lien. Cela vous révèle la vraie destination de l'endroit sur lequel vous arriverez si vous cliquez sur le lien. Si la vraie destination est différente de celle apparaissant dans le courriel, cela indique une attaque.

F **MÉFIEZ-VOUS DES PIÈCES JOINTES.** N'ouvrez que celles que vous attendez.

! Méfiez-vous de tout message qui semble **TROP BEAU POUR ÊTRE VRAI.** (Non, vous ne venez pas de gagner à la loterie.)

!! Ce n'est pas parce que vous recevez un **COURRIEL D'UN AMI** que cela signifie que votre ami vous l'a envoyé. L'ordinateur de votre ami a pu être infecté ou son compte peut avoir été compromis. Si vous recevez un courriel suspect d'un ami ou d'un collègue de confiance, appelez-le par téléphone.

Si vous croyez avoir reçu un courriel frauduleux, transférez-le à l'adresse **fraudes@lacapitale.com**