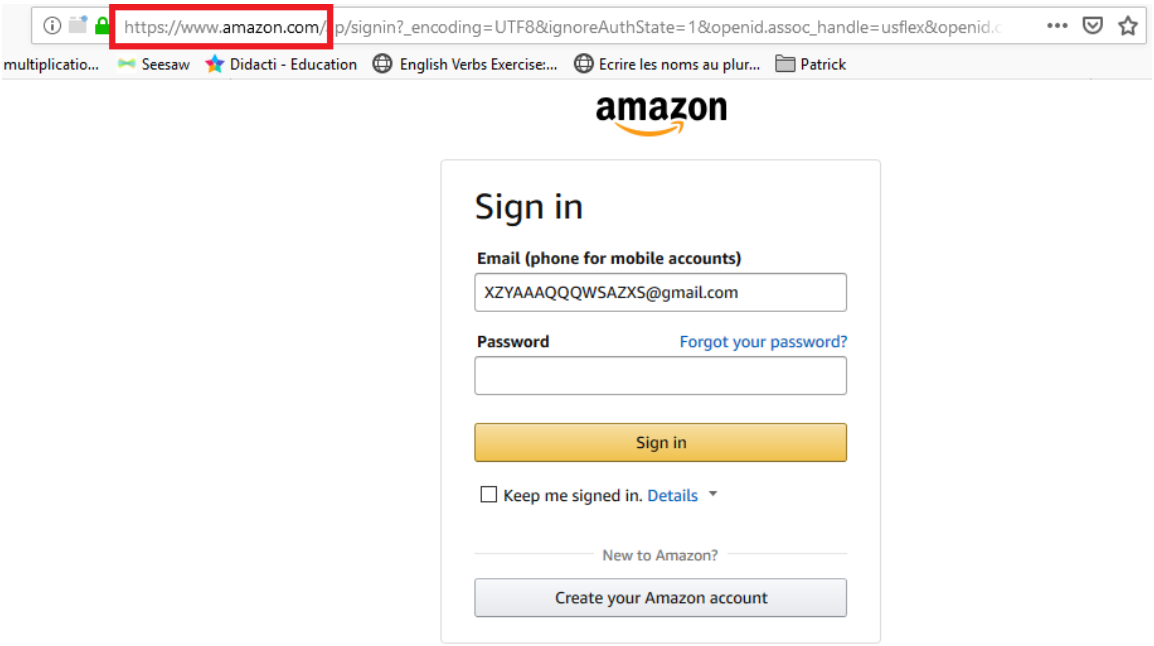
Éviter de se faire dérober ses accès

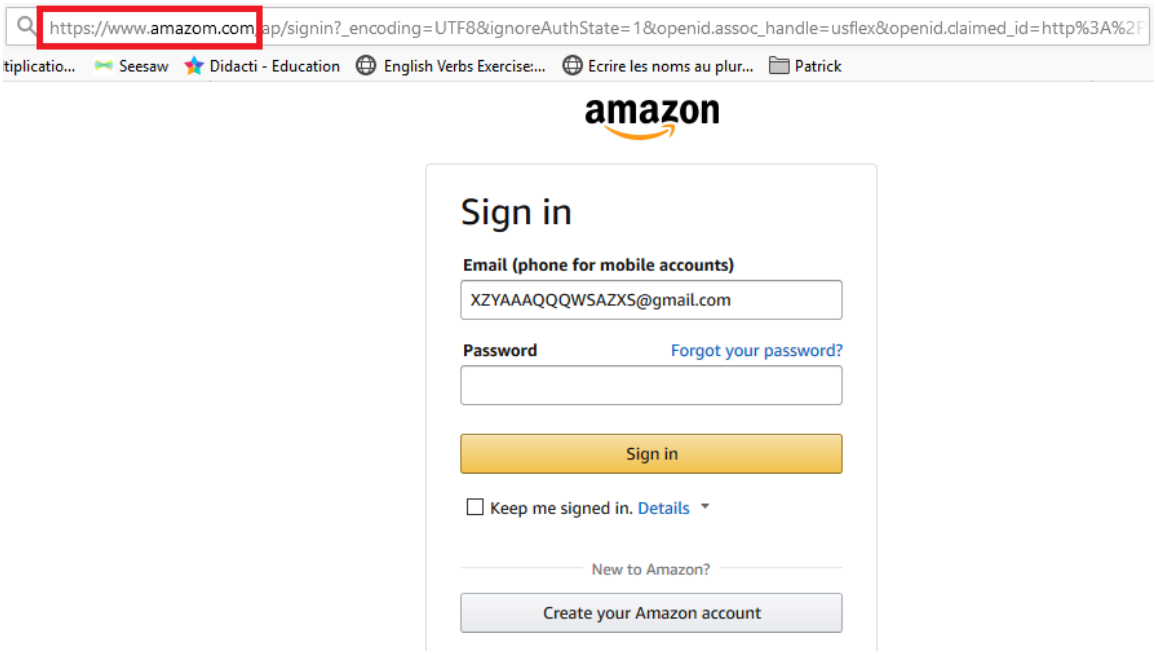
Texte de Patrick Sentinel – 29A

Se faire usurper son nom d'utilisateur et son mot de passe rend tout utilisateur un peu nerveux. Personne ne désire voir un pirate informatique se servir de ses accès! Les suggestions qui suivent pourraient vous aider à éviter le problème.

Lorsque nous nous rendons sur un site quelconque, nous ne prenons pas toujours le temps de confirmer l'exactitude des informations se trouvant dans la barre d'adresse (l'URL). Assurez-vous de vérifier le nom du domaine auquel vous désirez accéder. Par exemple, si vous allez sur Amazon, assurez-vous que l'URL est bien www.amazon.com avant de tenter de vous connecter. L'image suivante présente le véritable site avec la fenêtre de connexion.



Vous pouvez par ailleurs recevoir un courriel suspicieux qui vous demande de vous connecter à une application. Celle-ci est visuellement identique au site original, mais elle comporte une adresse différente et contient un comportement malicieux. L'utilisateur non attentif peut donc se faire dérober ses accès (nom d'utilisateur et mot de passe) s'il ne porte pas attention au contenu de la barre d'adresse dans le haut du navigateur. Dans notre exemple, l'URL du site original est www.amazon.com, alors que le site frauduleux est www.amazom.com. Il n'y a qu'une lettre qui différencie les URL, ce qui peut facilement tromper l'œil. Soyez vigilant!



En vérité, lorsque vous tentez de vous connecter au faux site à partir de l'interface utilisateur, vous entrez votre nom d'utilisateur et votre mot de passe. Vos informations seront enregistrées dans une base de données et seront désormais accessibles au malfaiteur. La personne mal intentionnée peut se connecter à votre insu et effectuer des transactions en vous laissant le soin de porter la responsabilité des transactions 😟 *This is crap*! Assurez-vous donc que l'URL que vous tapez dans la barre d'adresse est la bonne et sachez reconnaître le véritable site.

Une bonne façon d'éviter de se faire prendre est d'avoir en mémoire les URL auxquelles on veut accéder. Par exemple, si je désire aller sur le site eBay, je n'effectuerai pas de recherche pour accéder au site. Je taperai plutôt dans la barre d'adresse www.ebay.com et je m'assurerai que je tape la bonne URL avant de me connecter.

Lorsque vous recevez des courriels comportant des liens, ne cliquez pas sur le champ à moins d'être certain que les liens proviennent d'une source fiable à 100 %. Le bon vieux proverbe *Dans le doute mieux vaut s'abstenir* devrait être une référence lorsqu'on accède à une application qui exige le nom d'utilisateur et le mot de passe.

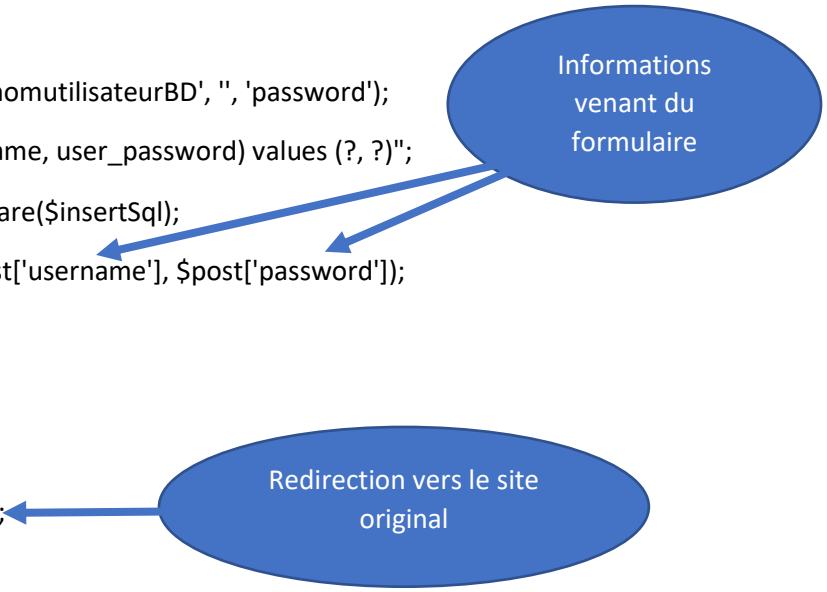
Fonctionnement du piège

Tout d'abord, le nom de domaine ressemble beaucoup à l'original. Dans le précédent exemple, on voyait www.amazom.com plutôt que www.amazon.com. Dans la barre d'adresse, on peut facilement les confondre si on ne regarde pas attentivement. De plus, l'apparence du site est identique à l'original, on n'y voit pas de différence.

Le malfaiteur ajoute du code malicieux et effectue une redirection pour donner l'impression que l'utilisateur a effectué une erreur lors de sa tentative de connexion. **Puisque la redirection pointe directement vers le site original, l'utilisateur est alors convaincu qu'il a d'abord tenté d'accéder au site original.**

Script php pouvant effectuer le travail :

```
$post = $_POST;
$dbConnection = new mysqli('amazom', 'nomutilisateurBD', '', 'password');
$insertSql = "insert into accounts (user_name, user_password) values (?, ?)";
$insertStatement = $dbConnection->prepare($insertSql);
$insertStatement->bind_param("ss", $post['username'], $post['password']);
$insertStatement->execute();
$insertStatement->close();
$dbConnection->close();
header("Location: https://amazon.com/");
```



C'est une arnaque à laquelle il faut porter attention! **Lorsque vous recevez un courriel qui contient un lien pour vous connecter, il est important de ne JAMAIS cliquer sur ce lien (à moins d'être certain que le lien est valide).** Tapez plutôt l'URL du site dans la barre d'adresse.