

1. Les attaques MITM
2. Le phishing
3. Les attaques CSRF
4. Les modifications du DOM
5. Les injections
6. Le brute force

# LE PHISHING

Avez-vous déjà entendu parler  
de phishing ?



Les adeptes de l'hameçonnage envoient habituellement **des courriels à un grand nombre de victimes.**

Typiquement, les messages ainsi envoyés **semblent émaner d'une société digne de confiance** et sont formulés de manière à alarmer le destinataire afin qu'il effectue une action en conséquence.

Une approche souvent utilisée est d'indiquer à la victime que son compte a été désactivé à cause d'un problème et que la réactivation ne sera possible qu'en cas d'action de sa part.

Le message fournit alors un lien internet qui dirige l'utilisateur vers une page Web qui **ressemble à s'y méprendre au vrai site** de la société digne de confiance. Arrivé sur cette page falsifiée, l'utilisateur est invité à saisir des **informations confidentielles qui sont alors enregistrées par le criminel.**



# Le Jeu du siècle : Qu'est-ce qui cloche ?





Re: 2e tentative pour Laurence



**E. Leclerc** <info@nlntgs.org.us>

07:51 (il y a 2 heures)



À moi ▾

# E.Leclerc

OPPORTUNITÉ À DURÉE LIMITÉE

**Votre adresse a été choisie  
pour obtenir un cadeau**

**Veuillez remplir simplement notre  
questionnaire en 1 min sur E.Leclerc, pour  
profiter de cette offer speciale.**

**COMMENCER** ▶

Si vous préférez ne plus recevoir de futurs e-mails, [Se désabonner ici](#).

# Roulement de tambours ...



Police étrange

Re: 2e tentative pour Laurence

Email étrange

E. Leclerc

<info@nlntvgs.org.us>

07:51 (il y a 2 heures)

Formulation  
souvent  
utilisée en  
phishing

E.Leclerc

OPPORTUNITÉ À DURÉE LIMITÉE

Votre adresse a été choisie

pour obtenir un un cadeau

Veuillez remplir simplement notre  
questionnaire en 1 min sur E.Leclerc, pour  
profiter de cette offer speciale.

COMMENCER ▶

Si vous préférez ne plus recevoir de futurs e-mails, [Se désabonner ici](#).

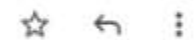
Les emails de phishing peuvent être très **convaincants** car ils peuvent avoir un niveau de personnalisation élevé !

Ils peuvent inclure notre nom, le nom d'une personne de notre famille etc.

Re:Bonne journée 🔥



Susan DOE <aguirre.christopher.barabra@hotmail.com> 3 août 2021 08:06 (il y a 9 jours)



À arnaudboulliung, moi, Nathalie, Emilie, nidaa ▾

Je ne sais pas quoi dire <https://bit.ly/3llk9Ss>

Susan DOE 🇧🇪

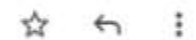
# Le Jeu du siècle : Qu'est-ce qui cloche ?



Re:Bonne journée 🔥



Susan DOE <aguirre.christopher.barabra@hotmail.com> 3 août 2021 08:06 (il y a 9 jours)



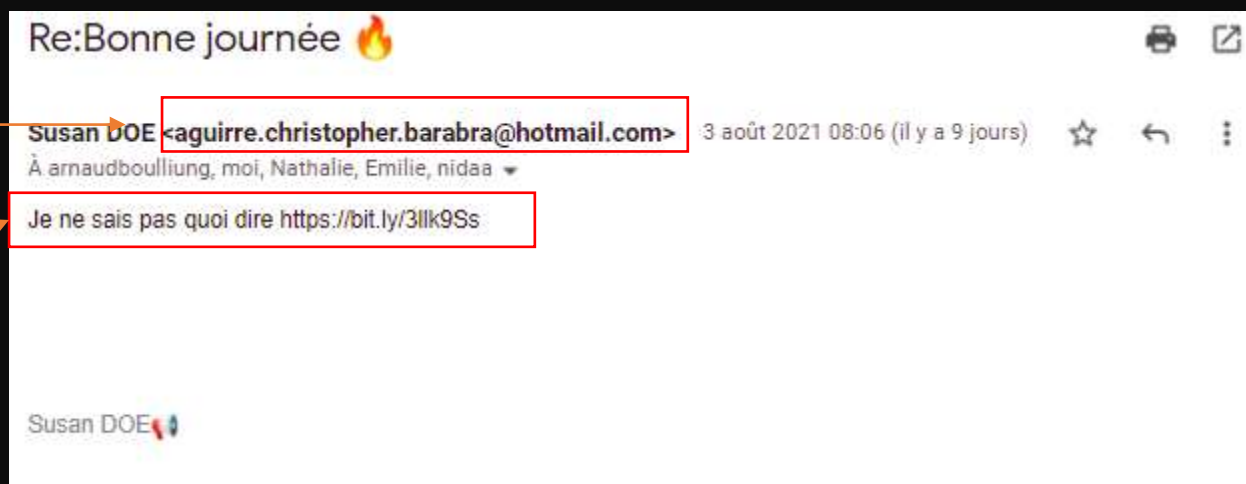
À arnaudboulliung, moi, Nathalie, Emilie, nidaa ▾

Je ne sais pas quoi dire <https://bit.ly/3llk9Ss>

Susan DOE 🇧🇪

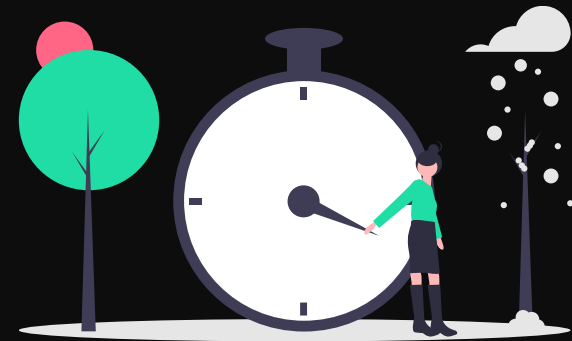
Email étrange

Corps de mail  
étrange





Comment le hacker a eu le nom  
de ma soeur ?



Car elle a du installer une application et  
cette application **a demandé la**  
**permission** d'accéder aux données et  
elle l'a accepté

Est-ce que vous lisez les  
demandes de permissions de  
vos applications ?



Il faudrait ! =)

# Il faudrait ! =)

Cela permet de s'assurer que vos données ne sont pas accessibles par n'importe quelle application et plus tard, utilisées à des fins de hacking



A LA PLACE D'UN HACKER ...

## Objectifs :

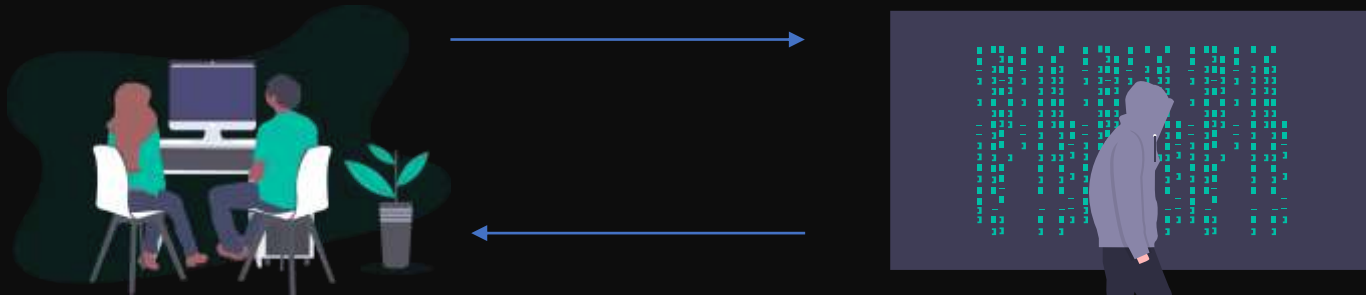
1. Voler des informations confidentielles (comme les identifiants et le mot de passe d'un compte bancaire)

## Mise en place :

1. Créer un faux site qui ressemble à un vrai site
2. Ecrire un email qui ressemble à un vrai et l'envoyer à un maximum de personnes



bnpparibas-connect.fr  
(fake)



Le hacker enregistre les  
données pour les utiliser  
plus tard

