

Le Phishing





Le **Phishing** ou **Hameçonnage**

- ⦿ Récupérer des **données personnelles**
- ⦿ Se faire passer pour une **personne**, un **site** ou un **service**
- ⦿ Copie **visuelle** et/ou **comportementale** d'une entité
- ⦿ Profite de diverses circonstances (événements, périodes de l'année...etc)



Le **Phishing** - démonstration 1

The screenshot shows a web browser window with the address bar displaying `https://www.faccbook.com/`. The page has a blue header with the Facebook logo on the left and a login section on the right. The login section includes a text input field for 'Adresse e-mail ou mobile', a 'Connexion' button, and a checkbox for 'Garder ma session active'. Below the header, the main content area features the text 'Avec Facebook, partagez et restez en contact avec votre entourage.' followed by a graphic of a network map with orange user icons connected by dashed lines. On the right side, there is a large 'Inscription' heading and the text 'C'est gratuit (et ça le', followed by input fields for 'Prénom' and 'Numéro de mobile ou'.

facebook

Adresse e-mail ou mobile

Connexion

☐ Garder ma session active

Avec Facebook, partagez et restez en contact avec votre entourage.

Inscription

C'est gratuit (et ça le

Prénom

Numéro de mobile ou



Le **Phishing** – démonstration 2

free BIENVENUE DANS VOTRE **ESPACE ABONNÉ**

 Accueil

ABONNÉ FREE MOBILE
IDENTIFIEZ-VOUS

- » Accédez à vos suivis commandes
- » Gardez un œil sur vos consommations
- » Gérez vos options
- » Commandez vos mobiles

UNE QUESTION ?
CONSULTEZ L'ASSISTANCE

Veuillez saisir votre identifiant grâce aux touches ci-dessous :

0	9	8	7	4
6	3	1	2	5

Identifiant : **Utilisez le pavé numérique ci-dessus.**

Mot de passe :

Vous avez oublié votre mot de passe ou perdu vos identifiants ?

[> AIDE VOCALE DÉSACTIVÉE](#)

assistance-mobilefree.com/facture/d08828b19f2f20871e3b83fef6178/moncompte/index.php?clientid=136896



Le **Phishing** – démonstration 3

Démonstration du tab-nabbing

Credits : *Aza Raskin*



Le **Spear Phishing**

- ⦿ Attaque **directe** et très **ciblée** envers un individu
- ⦿ Le contenu **concerne directement** la future victime
- ⦿ Demande une bonne connaissance de la cible
- ⦿ Plus efficace que la méthode classique



Le **Phishing in-session**

- ◉ Utilise un code *JavaScript* détectant un site **connu**
- ◉ Lance un message d'alerte **à l'intérieur du site**
- ◉ Très difficile à détecter pour la victime
- ◉ Mais plus rare (difficile à mettre en place)



Le **Pharming**

- ⦿ Redirection de trafic depuis un site connu vers un site pirate
- ⦿ Soit en exploitant des vulnérabilités DNS
- ⦿ Soit via un programme modifiant les paramètres réseaux



Contre-mesures

- ◉ Vérifier **les informations de l'expéditeur**
- ◉ Vérifier la présence **d'erreurs ou de fautes d'orthographe**
- ◉ Connaître les **vraies pratiques** des entreprises
- ◉ Sensibiliser le personnel et s'assurer de l'assimilation de la **politique**
- ◉ Netcraft, phishtank. Internetsignalement. WOT, SE toolkit, dkim spf