Chapitre3 : les fléaux de l'Internet

I. Introduction générale

Internet : un outil puissant mais risqué

Internet facilite la communication, l'accès à l'information, mais il expose aussi les utilisateurs à des menaces :

- Logiciels malveillants,
- Arnaques,
- Atteintes à la vie privée,
- Vol d'informations personnelles ou bancaires.

On appelle fléaux d'Internet l'ensemble de ces nuisances numériques.

II. La diffusion de virus informatiques

1. Définition

Un **virus informatique** est un programme malveillant capable de se reproduire et de se propager d'un ordinateur à un autre

Modes de propagation

- Pièces jointes d'emails infectées
- Clés USB ou disques externes
- Téléchargements illégaux ou non sécurisés
- Sites web compromis

2. Conséquences

- Ralentissement du système
- Suppression ou chiffrement de fichiers
- Vol de données personnelles
- Blocage complet de l'appareil (cas du ransomware)

3. Exemples connus

- **ILOVEYOU (2000)** : virus envoyé par e-mail, a contaminé des millions d'ordinateurs.
- **WannaCry (2017)** : ransomware qui a paralysé des hôpitaux et entreprises.

4. Moyens de protection

- Utiliser un antivirus à jour
- Ne jamais ouvrir une pièce jointe suspecte
- Faire régulièrement les mises à jour du système
- Sauvegarder ses données sur un support externe ou cloud sécurisé

III. L'envahissement de la boîte aux lettres (le spam)

1. Définition

Le **spam** est l'envoi massif de messages non sollicités, souvent à but publicitaire ou frauduleux.

2. Formes de spam

- **Publicité indésirable** : produits, services, sites douteux
- **Phishing (hameçonnage)** : emails qui imitent des sites officiels (banque, administration) pour voler vos données

  Le phishing, ou hameçonnage, est une technique frauduleuse où un cybercriminel se fait passer pour une entité de confiance (banque, administration, entreprise) pour voler des informations personnelles et/ou bancaires
- **Chaînes ou fausses alertes** : messages à transférer, souvent porteurs de liens dangereux

3. Conséquences

- Saturation de la boîte mail
- Perte de temps
- Risques d'infection ou de fraude

4. Moyens de protection

- Activer les **filtres anti-spam** du fournisseur de messagerie
- Ne pas cliquer sur les liens d'emails suspects
- Ne jamais répondre à un spam (cela confirme votre adresse)
- Utiliser une **adresse secondaire** pour les inscriptions sur Internet

IV. L'irruption de pop-up et les publicités malveillantes

1. Définition

Les **pop-ups** sont de petites fenêtres qui s'ouvrent automatiquement lors de la navigation.
Certaines sont légitimes (ex. connexion ou formulaire), mais d'autres sont **malveillantes**.

2. Dangers des pop-ups malveillantes

- Téléchargement de programmes indésirables (adware, spyware)
- Collecte d'informations personnelles
- Redirection vers des sites frauduleux

3. Moyens de protection

- Activer le **bloqueur de pop-up** du navigateur

- Éviter les sites non sécurisés (adresse sans “https://”)
- Installer une **extension de protection publicitaire (Ad Block, uBlock)**
- Maintenir le navigateur à jour

V. La fraude à la carte bancaire sur Internet

1. Définition

La **fraude bancaire en ligne** consiste à utiliser les données de carte bancaire d’une personne sans son autorisation, souvent à la suite d’un vol d’informations.

2. Méthodes de fraude les plus fréquentes

1. **Phishing** : faux email ou faux site qui imite votre banque.

   Principe : Les escrocs usurpent l'identité d'organismes de confiance (banque, administration, etc.) pour inciter la victime à divulguer des informations sensibles (mots de passe, données bancaires) via de faux emails, SMS ou sites web.

   Exemple : Un faux e-mail de votre banque qui vous demande de vous connecter à votre compte via un lien pour "sécuriser une opération".

2. **Skimming** : copie des données de la carte à l’aide d’un lecteur frauduleux.

   Principe : Un dispositif frauduleux est installé sur un distributeur de billets ou un terminal de paiement pour copier les données de la carte et/ou enregistrer votre code confidentiel.

   Exemple : Un faux lecteur de carte inséré sur un distributeur automatique, ou un clavier piraté qui enregistre votre code lors de sa saisie.

3. **Pirate informatique** interceptant les données lors d’un paiement en ligne non sécurisé.

   Principe : Le pirate intercepte les données bancaires lors d'une transaction sur un réseau Wi-Fi public ou peu sécurisé.

   Exemple : Vous utilisez le Wi-Fi de l'aéroport pour faire un achat en ligne et un pirate sur le même réseau parvient à capter les informations de votre carte.

3. Conséquences

- Vol d’argent
- Blocage de la carte bancaire
- Démarches administratives longues

4. Moyens de protection

- Vérifier que le site est sécurisé (https://)

- Ne jamais communiquer son code secret ou les 3 chiffres du dos de la carte par email
- Utiliser les systèmes de **paiement sécurisés** (3D Secure, PayPal, cartes virtuelles)
- Surveiller régulièrement ses relevés bancaires

VI. . Bonnes pratiques générales

	Comportement		Objectif
	Mettre à jour ses logiciels et son antivirus		Éviter les failles exploitées par les pirates
	Utiliser des mots de passe forts et différents		Protéger ses comptes
	Sauvegarder régulièrement ses données		Réduire les pertes en cas d'attaque
	Être vigilant face aux emails ou offres trop alléchantes		Éviter les arnaques
	Naviguer sur des sites fiables et connus		Réduire les risques de fraude

VII. Conclusion

Internet n'est pas dangereux en soi, mais l'imprudence l'est.
Les virus, le spam, les pop-ups et la fraude bancaire représentent les menaces les plus courantes.
Grâce à la vigilance, la mise à jour des logiciels et une bonne hygiène numérique, chacun peut s'en protéger efficacement.