

Sécurité des Réseaux



Plan général

1. Quelques rappels

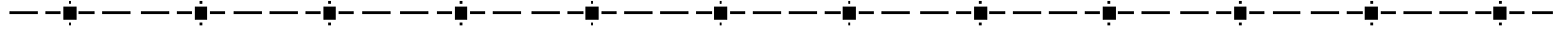
- ◆ Sur Internet /réseau
- ◆ Sur les équipements
- ◆ Sur le vocabulaire et les types d'attaque

2. Sécurité des accès

- ◆ Filtrage
- ◆ Utilisation de parefeu

3. Sécurité des échanges

- ◆ PKI
- ◆ IPsec



Introduction

Quelques chiffres sur Internet (1)

JAN 2024

DIGITAL GROWTH

CHANGE IN THE USE OF CONNECTED DEVICES AND SERVICES OVER TIME



GLOBAL DATA

TOTAL POPULATION



+0.9%

YEAR-ON-YEAR CHANGE
+74 MILLION

Meltwater

UNIQUE MOBILE PHONE SUBSCRIBERS



+2.5%

YEAR-ON-YEAR CHANGE
+138 MILLION

Kepios

INDIVIDUALS USING THE INTERNET



+1.8%

YEAR-ON-YEAR CHANGE
+97 MILLION

we are social

SOCIAL MEDIA USER IDENTITIES



+5.6%

YEAR-ON-YEAR CHANGE
+266 MILLION

OCT 2018

DIGITAL AROUND THE WORLD IN OCTOBER 2018

THE LATEST STATISTICAL INDICATORS FOR INTERNET, SOCIAL MEDIA, AND MOBILE USE AROUND THE WORLD

TOTAL POPULATION



7.655

BILLION

URBANISATION:
55%

INTERNET USERS



4.176

BILLION

PENETRATION:
55%

ACTIVE SOCIAL MEDIA USERS



3.397

BILLION

PENETRATION:
44%

UNIQUE MOBILE USERS



5.118

BILLION

PENETRATION:
67%

ACTIVE MOBILE SOCIAL USERS



3.179

BILLION

PENETRATION:
42%

we are social

we are social

we are social

we are social

we are social

SOURCES: POPULATION: UNITED NATIONS, U.S. CENSUS BUREAU, INTERNET: INTERNET WORLDSTATS, ITA, EUROSTAT, INTERNETLIVESTATS, CIA WORLD FACTBOOK, MIDEASTMEDIA.ORG, FACEBOOK, GOVERNMENT OFFICIALS, REGULATORY AUTHORITIES, REPUTABLE MEDIA, SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK, TENCENT, WIKITRAKE, KAKAO, NAVER, DING, TECHRADA, SIMILARWEB, KEPIOS ANALYSIS; MOBILE: GSM, INTELLIGENCE, GOOGLE, ERICSSON, KEPIOS ANALYSIS. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).

Hootsuite we are social

JAN 2024

ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

TOTAL POPULATION



8.08
BILLION

URBANISATION
57.7%

we are social

UNIQUE MOBILE PHONE SUBSCRIBERS



5.61
BILLION

vs. POPULATION
69.4%

Meltwater

INDIVIDUALS USING THE INTERNET



5.35
BILLION

vs. POPULATION
66.2%

Kepios

SOCIAL MEDIA USER IDENTITIES



5.04
BILLION

vs. POPULATION
62.3%

Kepios

JAN 2024

FRANCE

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MEAN THAT FIGURES SHOWN HERE ARE NOT COMPARABLE WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.

TOTAL POPULATION



64.82
MILLION

YEAR-ON-YEAR CHANGE
+0.2%
+128 THOUSAND

URBANISATION
81.9%

we are social

CELLULAR MOBILE CONNECTIONS



75.02
MILLION

YEAR-ON-YEAR CHANGE
+0.7%
+528 THOUSAND

TOTAL vs. POPULATION
115.7%

Meltwater

INDIVIDUALS USING THE INTERNET



60.80
MILLION

YEAR-ON-YEAR CHANGE
+0.2%
+120 THOUSAND

TOTAL vs. POPULATION
93.8%

Meltwater

SOCIAL MEDIA USER IDENTITIES



50.70
MILLION

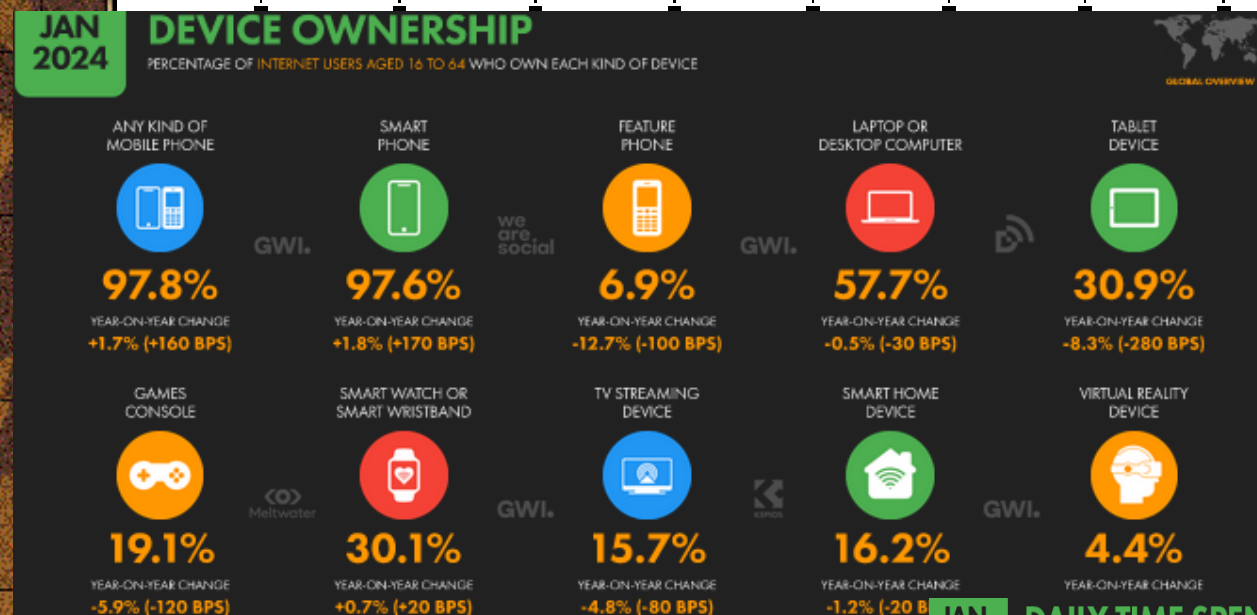
YEAR-ON-YEAR CHANGE
-2.7%
-1.4 MILLION

TOTAL vs. POPULATION
78.2%

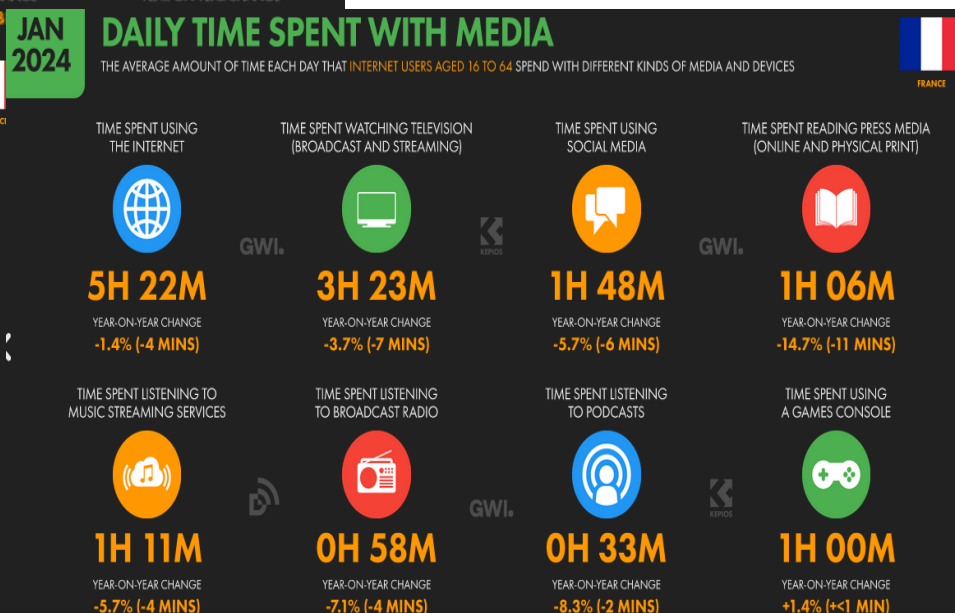
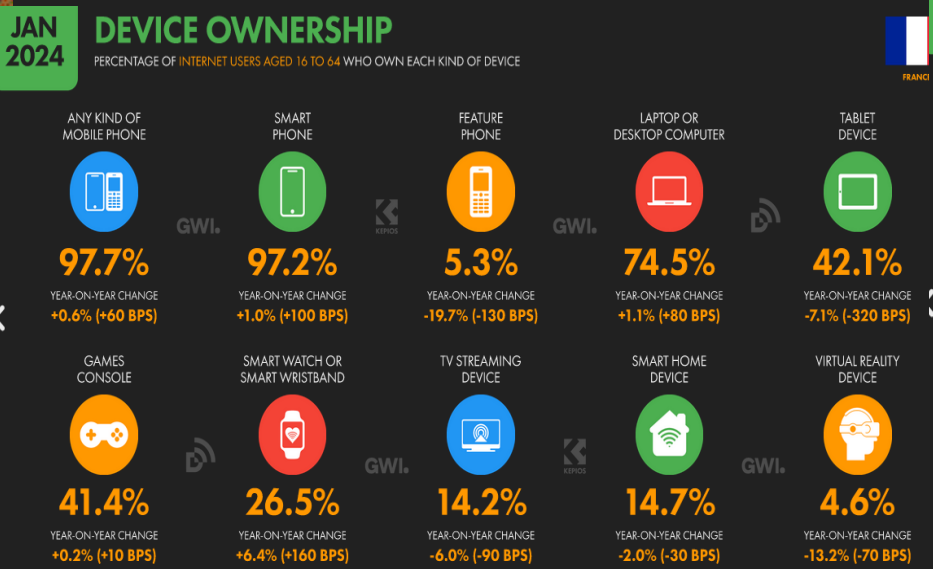
FRANCE

Hootsuite we are social

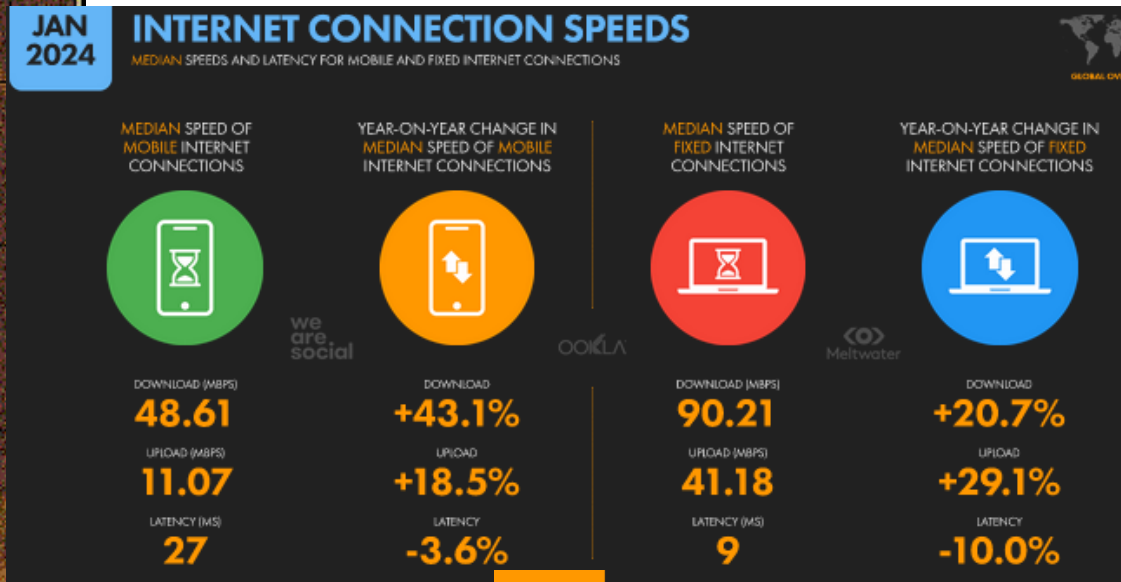
Quelques chiffres sur Internet (2)



Différents équipements pour aller sur internet



Quelques chiffres sur Internet (3)



Connexion de plus en plus rapide

Les réseaux sociaux sont très actifs (moyenne 2h23), inscrit sur 6 plateformes différentes

France :

79,66 Mbps mobile

207,41 Mbps fixe

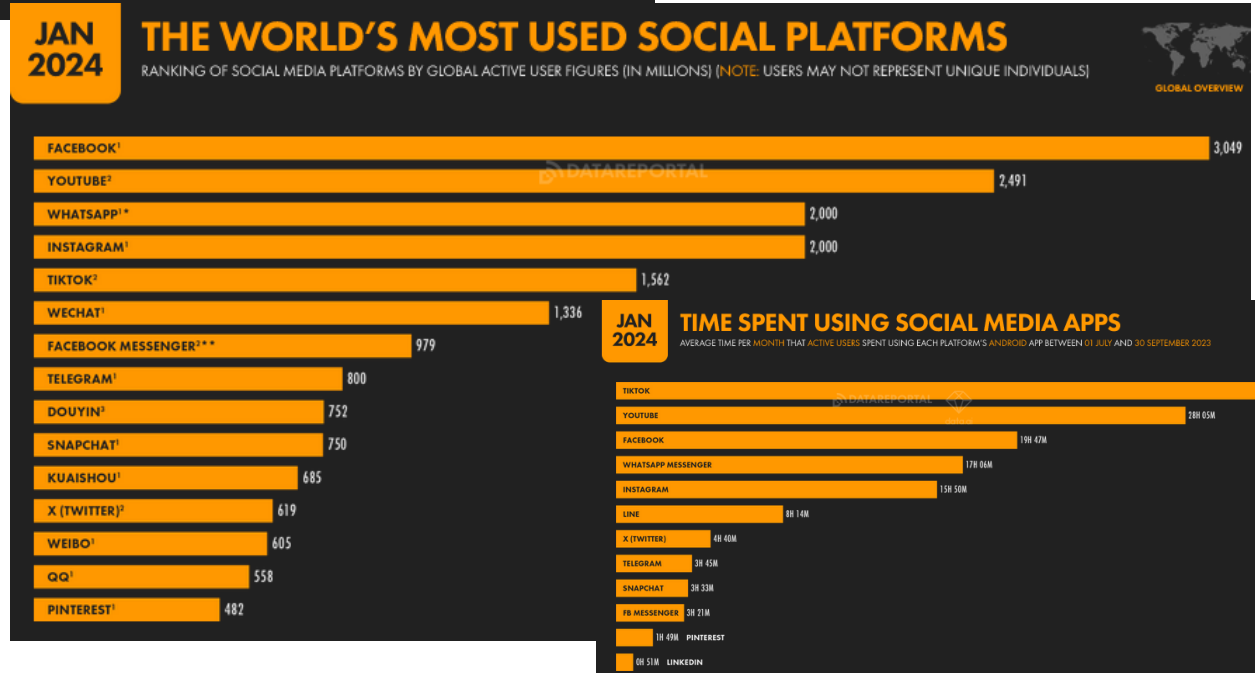
U.A.E : 324 Mbps

Singapore : 263 Mbps

Cuba : 3,9 Mbps

Cuba : 2,11 Mbps

©wearesocial.com



Quelques chiffres sur Internet (4)

JAN 2024

MOBILE CONNECTIVITY

ADOPTION AND USE OF MOBILE PHONES AND DEVICES THAT CONNECT TO CELLULAR NETWORKS

JAN 2024

SHARE OF MOBILE TIME BY APP CATEGORY

TIME SPENT USING APPS IN EACH APP CATEGORY AS A PERCENTAGE OF TOTAL TIME SPENT USING ANDROID PHONES OVERALL

NUMBER OF UNIQUE MOBILE SUBSCRIBERS (ANY TYPE OF HANDSET)



5.61
BILLION



UNIQUE MOBILE SUBSCRIBERS AS A PERCENTAGE OF TOTAL POPULATION



69.4%
YOY: +1.6% (+108 BPS)



ANNUAL CHANGE IN THE NUMBER OF UNIQUE MOBILE SUBSCRIBERS



+2.5%
+138 MILLION



AVERAGE NUMBER OF MOBILE CONNECTIONS PER UNIQUE MOBILE SUBSCRIBER



1.54
YOY: -0.6%



TOTAL TIME SPENT USING SMARTPHONES EACH DAY



5H 01M
YOY: +5.6% (+16 MINS)



SHARE OF SMARTPHONE TIME: SOCIAL MEDIA APPS



34.7%



SHARE OF SMARTPHONE TIME: ENTERTAINMENT APPS



31.4%



SHARE OF SMARTPHONE TIME: UTILITY & PRODUCTIVITY



14.4%

CELLULAR MOBILE CONNECTIONS (EXCLUDING IOT)



8.65
BILLION



ANNUAL CHANGE IN THE NUMBER OF CELLULAR CONNECTIONS (EX. IOT)



+1.9%
+160 MILLION



TOTAL NUMBER OF BROADBAND MOBILE CONNECTIONS



7.98
BILLION



NUMBER OF BROADBAND MOBILE CONNECTIONS AS A PERCENTAGE OF TOTAL MOBILE CONNECTIONS



92.3%
YOY: +3.8% (+339 BPS)



SHARE OF SMARTPHONE TIME: MOBILE GAMES (ALL GENRES)



11.1%



SHARE OF SMARTPHONE TIME: SHOPPING APPS



1.5%



SHARE OF SMARTPHONE TIME: ALL OTHER APPS



6.8%



SHARE OF SMARTPHONE TIME: WEB BROWSERS & SEARCH ENGINES*



6.3%

JAN 2024

MOBILE APPS: TOP CATEGORIES BY APP STORE

RANKING OF THE MOST POPULAR MOBILE APP CATEGORIES BETWEEN 01 SEPTEMBER AND 30 NOVEMBER 2023

JAN 2024

EVOLUTION OF MOBILE DATA CONSUMPTION

AVERAGE GLOBAL MOBILE DATA TRAFFIC (UPLOAD & DOWNLOAD) IN EXABYTES* PER MONTH

GOOGLE PLAY: DOWNLOADS

GOOGLE PLAY: CONSUMER SPEND

IOS APP STORE: DOWNLOADS

IOS APP STORE: CONSUMER SPEND

APP CATEGORY

- TOOLS APPS
- CASUAL GAMES
- ACTION GAMES
- SIMULATION GAMES
- ENTERTAINMENT APPS
- PUZZLE GAMES
- FAMILY APPS
- FINANCE APPS
- ARCADE GAMES
- SOCIAL APPS

APP CATEGORY

- ROLE PLAYING GAMES
- STRATEGY GAMES
- CASUAL GAMES
- ENTERTAINMENT APPS
- ACTION GAMES
- PUZZLE GAMES
- SOCIAL APPS
- ADVENTURE GAMES
- CASINO GAMES
- PRODUCTIVITY APPS

APP CATEGORY

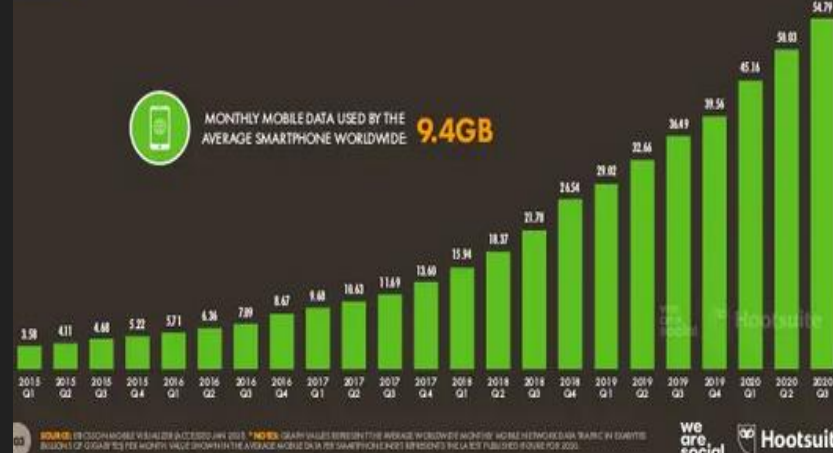
- UTILITIES APPS
- SHOPPING APPS
- CASUAL GAMES
- ENTERTAINMENT APPS
- PHOTO AND VIDEO APPS
- FINANCE APPS
- PRODUCTIVITY APPS
- LIFESTYLE APPS
- ACTION GAMES
- SOCIAL NETWORKING APPS

APP CATEGORY

- ROLE PLAYING GAMES
- STRATEGY GAMES
- ACTION GAMES
- ENTERTAINMENT APPS
- PUZZLE GAMES
- ADVENTURE GAMES
- SIMULATION GAMES
- CASUAL GAMES
- CARD GAMES
- PHOTO AND VIDEO APPS



MONTHLY MOBILE DATA USED BY THE AVERAGE SMARTPHONE WORLDWIDE **9.4GB**



Quelques chiffres sur Internet (5)

JAN
2024

ECOMMERCE: CONSUMER GOODS CATEGORIES

ESTIMATED ANNUAL SPEND IN EACH CONSUMER GOODS ECOMMERCE CATEGORY (B2C ONLY, U.S. DOLLARS, FULL-YEAR 2023)

GLOBAL OVERVIEW

ELECTRONICS



**\$781.3
BILLION**

YEAR-ON-YEAR CHANGE
+11.8% (+\$82 BILLION)

FASHION



**\$673.6
BILLION**

YEAR-ON-YEAR CHANGE
+8.4% (+\$52 BILLION)

FOOD



**\$370.7
BILLION**

YEAR-ON-YEAR CHANGE
+16.0% (+\$51 BILLION)

BEVERAGES



**\$209.3
BILLION**

YEAR-ON-YEAR CHANGE
+14.2% (+\$26 BILLION)

DIY & HARDWARE



**\$201.8
BILLION**

YEAR-ON-YEAR CHANGE
+8.5% (+\$16 BILLION)

FURNITURE



**\$188.0
BILLION**

YEAR-ON-YEAR CHANGE
+11.6% (+\$20 BILLION)

PHYSICAL MEDIA



**\$182.7
BILLION**

YEAR-ON-YEAR CHANGE
+0.8% (+\$1.5 BILLION)

BEAUTY &
PERSONAL CARE



**\$151.2
BILLION**

YEAR-ON-YEAR CHANGE
+5.1% (+\$7.4 BILLION)

TOBACCO
PRODUCTS



**\$104.4
BILLION**

YEAR-ON-YEAR CHANGE
+1.9% (+\$1.9 BILLION)

TOYS &
HOBBY



**\$80.53
BILLION**

YEAR-ON-YEAR CHANGE
+5.2% (+\$4.0 BILLION)

HOUSEHOLD
ESSENTIALS



**\$72.98
BILLION**

YEAR-ON-YEAR CHANGE
+11.9% (+\$7.8 BILLION)

OVER-THE-COUNTER
PHARMACEUTICALS



**\$59.65
BILLION**

YEAR-ON-YEAR CHANGE
+7.6% (+\$4.2 BILLION)

LUXURY
GOODS



**\$54.42
BILLION**

YEAR-ON-YEAR CHANGE
+9.7% (+\$4.8 BILLION)

EYE-
WEAR



**\$23.48
BILLION**

YEAR-ON-YEAR CHANGE
+5.9% (+\$1.3 BILLION)

©wearesocial.comv

JAN
2024

WEEKLY ONLINE SHOPPING ACTIVITIES

PERCENTAGE OF INTERNET USERS AGED 16 TO 64 WHO ENGAGE IN SELECTED ECOMMERCE ACTIVITIES EACH WEEK

PURCHASED A PRODUCT
OR SERVICE ONLINE



56.1%

YOY: -2.6% (-150 BPS)

ORDERED GROCERIES
VIA AN ONLINE STORE



28.2%

YOY: -0.4% (-10 BPS)

BOUGHT A SECOND-HAND
ITEM VIA AN ONLINE STORE



11.8%

YOY: -16.9% (-240 BPS)

USED AN ONLINE PRICE
COMPARISON SERVICE



20.6%

YOY: -12.3% (-290 BPS)

USED A BUY NOW,
PAY LATER SERVICE



16.0%

YOY: -13.0% (-240 BPS)



GLOBAL OVERVIEW

1. PROTÉGEZ VOS COMPTES AVEC DES MOTS DE PASSE ROBUSTES

2. SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT

3. FAITES SANS TARDER LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS

4. UTILISEZ UN ANTIVIRUS

5. SOYEZ PRUDENTS LORS DE VOS ACHATS EN LIGNE

6. MÉFIEZ-VOUS DES MESSAGES SUSPECTS

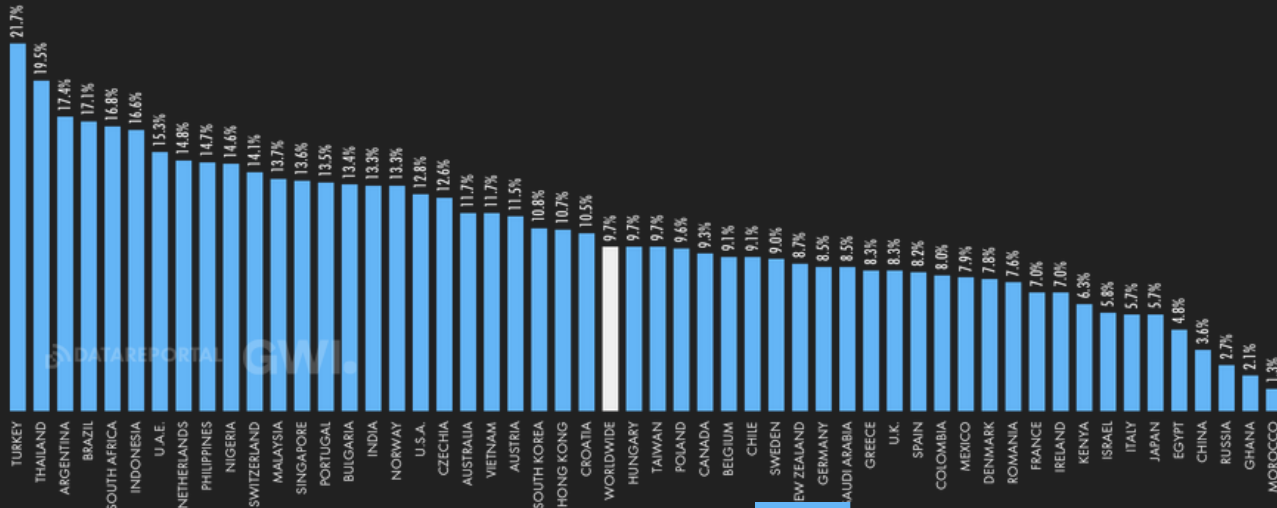
7. APPRENEZ À MAÎTRISER VOS RÉSEAUX SOCIAUX

Quelques chiffres sur Internet (6)

JAN 2024

OWNERSHIP OF CRYPTOCURRENCY

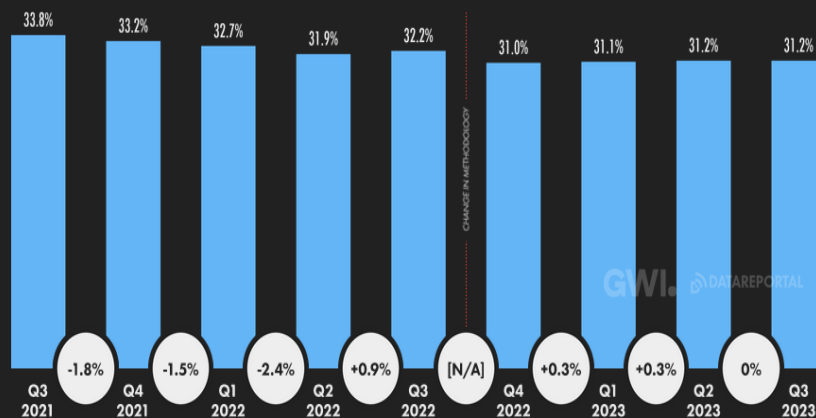
PERCENTAGE OF INTERNET USERS AGED 16 TO 64 WHO OWN SOME FORM OF CRYPTOCURRENCY



JAN 2024

CONCERNS ABOUT MISUSE OF PERSONAL DATA

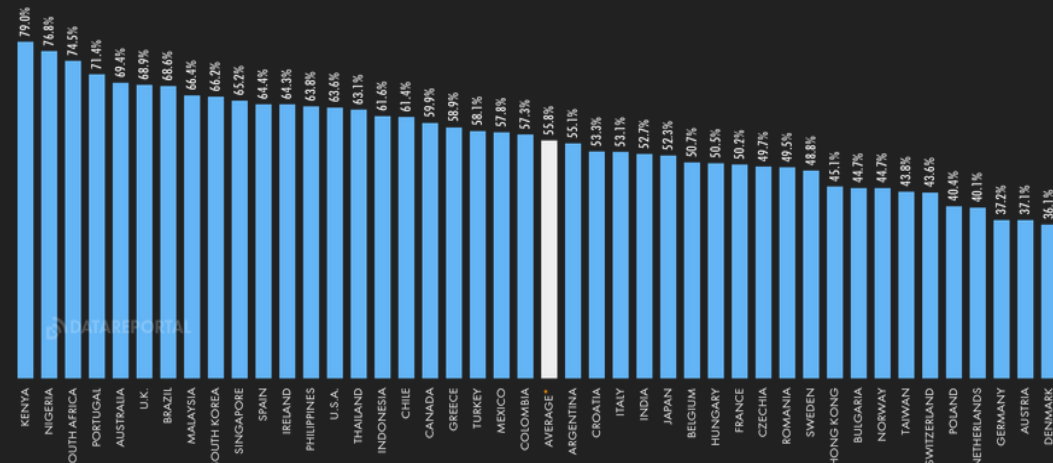
PERCENTAGE OF INTERNET USERS AGED 16 TO 64 WHO ARE WORRIED ABOUT HOW COMPANIES USE THEIR PERSONAL DATA ONLINE



JAN 2024

CONCERNS ABOUT ONLINE MISINFORMATION

PERCENTAGE OF ADULTS AGED 18+ WHO ARE CONCERNED ABOUT WHAT IS REAL OR FAKE ON THE INTERNET

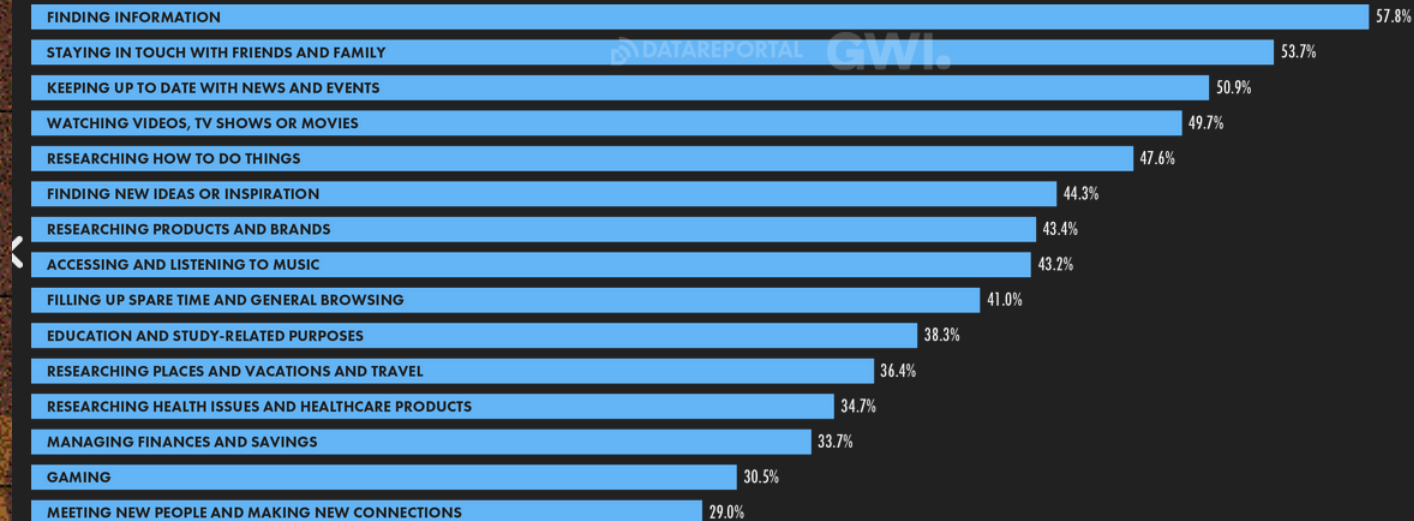


Internet

JAN
2023

MAIN REASONS FOR USING THE INTERNET

PRIMARY REASONS WHY INTERNET USERS AGED 16 TO 64 USE THE INTERNET



JAN
2023

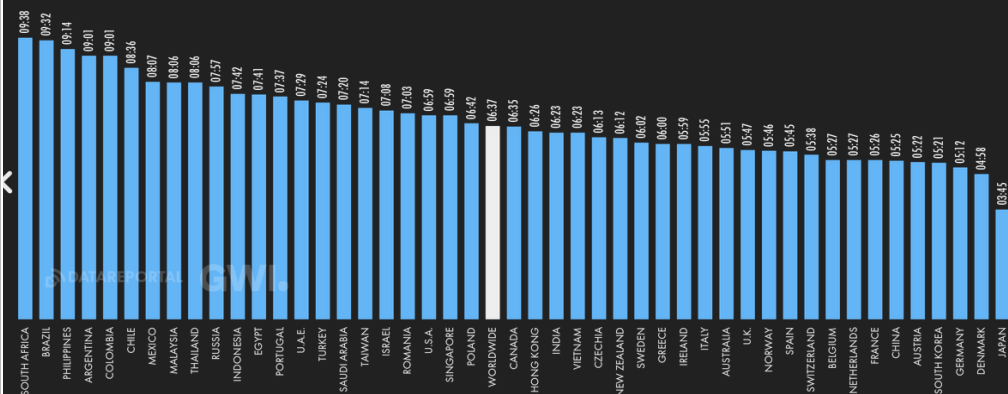
TOP WEBSITES: SEMRUSH R

SEMRUSH'S RANKING OF THE MOST VISITED WEBSITES, BASED ON WEBSITE TR

JAN
2023

DAILY TIME SPENT USING THE INTERNET

AVERAGE AMOUNT OF TIME (IN HOURS AND MINUTES) THAT INTERNET USERS AGED 16 TO 64 SPEND USING THE INTERNET EACH DAY ON ANY DEVICE



Des statistiques !!

- En moyenne, il faut **6 mois** à une entreprise pour détecter une violation de ses données (50000 euros, coût médian d'une cyberattaque)
- La plupart des domaines de nom malveillants (site ressemblant à un site connu), environs 60%, sont associés à des campagnes de spam.
- Les attaques de ransomware se produisent tous **les 10 secondes**.
- 54% des entreprises françaises attaquées en 2021.
- 41% des entreprises ont plus de 1 000 fichiers sensibles, y compris les numéros de carte de crédit et les dossiers médicaux, laissés sans protection.
- 94% de tous les logiciels malveillants est livré par e-mail.
- 65% des entreprises ont des utilisateurs qui ne modifient jamais leurs mots de passe.
- 69% des entreprises ne pensent pas que leur logiciel anti-virus puisse bloquer les menaces qu'elles détectent.
- 50% des structures victimes portent plainte

OWASP

Open Web Application Security project

- Authentification brisée - Broken access control
- Exposition de données sensibles (cryptographic failure)
- Injection SQL (y compris XSS)
- Insecure Design
- Security misconfigurations
- Using components with known vulnerabilities
- Identification and authentication failures
- Software and Data integrity Failures
- Insufficient logging and monitoring
- Server Side Request Forgery (SSRF)

Internet

✧ Internet : vecteur physique considérable de vulnérabilité

- ◆ Tous les réseaux sont connectés
- ◆ De plus en plus d'objets sont connectés en réseaux et accessibles
- ◆ Le commerce électronique est omniprésent
- ◆ Augmentation de la bande passante
- ◆ Les informations peuvent circuler très vite
- ◆ Le Time to Market diminue, au détriment des tests et de la sécurité des applications

✧ CERT

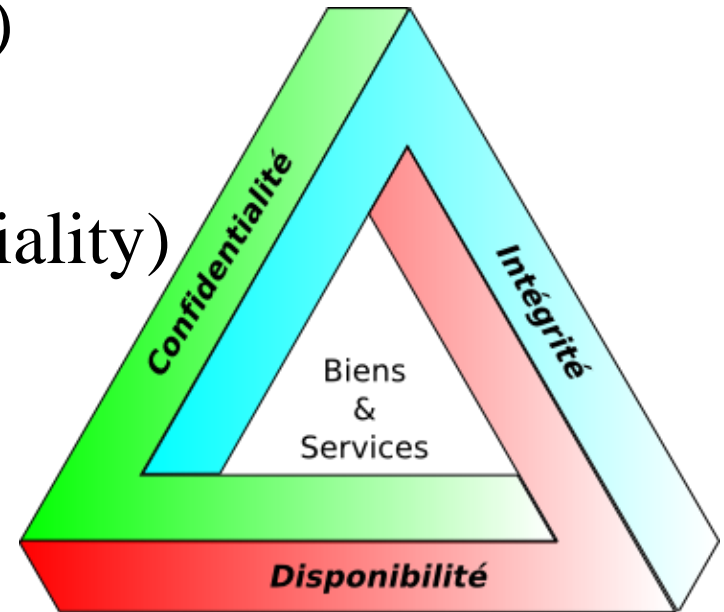
- ◆ Computer Emergency Response Team
- ◆ Met à jour la liste des attaques et les contre-mesures à appliquer

✧ CVE (Common Vulnerability and Exposure)

- ◆ Toutes les failles sont théoriquement répertoriées par ce site
- ◆ En inverse, possibilité de trouver des exploits (vuldb, exploit-db, etc...)

La Triade

- ✦ Disponibilité (availability)
- ✦ Intégrité (integrity)
- ✦ Confidentialité (confidentiality)



- ✦ Preuve
- ✦ Non-répudiation

 Contrôle des accès

Contrôle des accès

✦ 3 catégories

- ◆ Administratives (politique de sécurité)
 - Qui, où, comment, etc
- ◆ Technique/logiciel
 - Parefeu, identification, password, etc...
- ◆ Physique
 - Accès aux locaux, aux prises, etc..

➡ Nécessité de pouvoir vérifier le fonctionnement

- journalisation des actions
- Durée de conservation des logs

Identification/Authentication

✧ 2 concepts différents

✧ Authentication

◆ 4 facteurs possibles

- utiliser une information que seul le commettant connaît (ce que l'on connaît)
- utiliser une information unique que seul le commettant possède (ce que l'on possède)
- utiliser une information qui caractérise le commettant dans un contexte donné (ce que l'on est)
- utiliser une information que seul le commettant peut produire (ce que l'on sait faire).

◆ simple (1 facteur), forte(≥ 2 facteurs)

MFA – MULTI FACTOR AUTHENTICATION

◆ SSO (Single Sign-On) -> 1 seule authentification pour tout

Authentication(1)

✧ Password

◆ Sécurité faible

- Souvent simple, stockage ou transmission en clair, etc
- Augmentation de la difficulté en rajoutant des contraintes
- Limiter le nombre d'essais

✧ Biométrieque

- ◆ Empreinte digitale ou rétinienne, voix, main, faciale, etc..
- ◆ Problème faux positifs ou faux négatifs

✧ Carte à puce

- ◆ Clé statique ou dynamique

✧ Ticket

- ◆ Dédié pour kerberos

Rappel : le réseau

✦ Modèle en couches

- ◆ **Modèle OSI : 7 couches**
- ◆ **Modèle TCP/IP : 4 couches** → création 1973
- ◆ **Basé sur IP au niveau 3**
 - Mode non connecté, sans mécanisme de sécurité (IPv6 n'est pas encore beaucoup utilisé)
- ◆ **Basé sur TCP au niveau 4**
 - Fiable, assure la retransmission des paquets perdus et une gestion « simple » de la bande passante -> algorithme new Reno ou Cubic
- ◆ **Basé sur UDP au niveau 4**
 - Non fiable, non sécurisé
- ◆ **Niveau applicatif**
 - Protocole plus ou moins récent, sécurisé ou non

Les différentes adresses

✧ Au niveau 2

- ✧ Adresse MAC (adresse physique)
- ✧ Théoriquement fixe, unique sur le réseau local
- ✧ Quelques bibliothèques permettent de créer des trames directement à ce niveau (pcap, scapy)

✧ Au niveau 3

- ✧ Adresse IP (adresse logique)
- ✧ Adresse Privée/publique
- ✧ Change au gré des utilisateurs

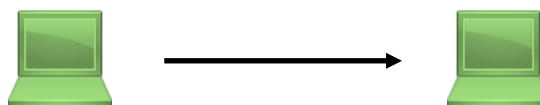
✧ Au niveau 4

- ✧ Port (réservé en-dessous de 1024)

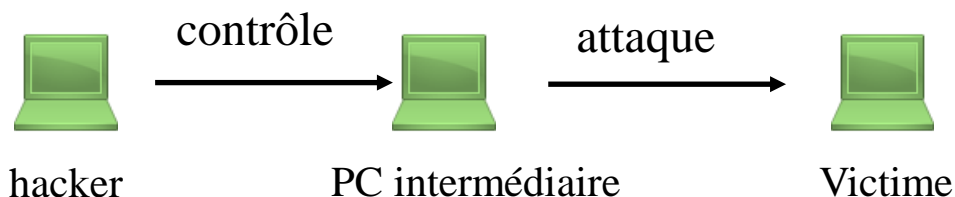
Si aucun port n'est ouvert, sécurité accrue, obligation de passer par le niveau 2 (même site)

Les différents types d'attaque

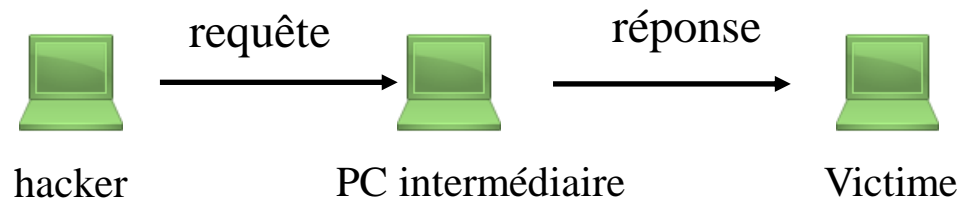
✦ Attaque directe



✦ Attaque indirecte par rebond



✦ Attaque indirecte par réponses



Cartographie du réseau (1)

✧ Renseignement sur le réseau

◆ Recherche d'informations publiques

- DNS, whois,
- Utilisation d'utilitaire (dig, host,)
- Test des chemins via traceroute/tracert (fonctionnement du TTL) , cheops-ng,
- Envoie d'un mail avec mauvais correspondant

◆ Balayage

- Découvrir les machines présentes
- Le protocole ICMP
- ICMPv6 a encore plus de fonctionnalités...
- Présence de filtrage (utilisation du TTL, et ICMP)
 - ◆ Logiciel firewall, nmap

Cartographie du réseau (2)

✧ Renseignement sur le réseau

◆ Balayage sur les ports

- Quels ports sont ouverts ?
- Envoie d'un paquet, et attente du retour
- Ex : envoie de syn sur un port,
 - ◆ Si retour = syn+ ack , port ouvert
 - ◆ Si retour= rst, port fermé
 - ◆ Si pas de retour, possibilité pare-feu.

◆ Logiciel nmap, netdiscover, netcat,

- Scan Half open syn, Null, xmas,.... (option de nmap)

Méthodes assez détectable.... Sauf si étalé dans le temps.

Attaque sur switch

✦ Augmentation de la sécurité : VLAN

- ◆ Protocole 802.1Q permet de simplifier la gestion/trunking

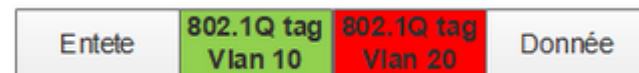
✦ Saut de VLAN

◆ Switch spoofing

- (utilisation du protocole Dynamic Trunk Protocol)
- Objectif : se faire passer pour un switch, puis configurer liaison trunk avec le switch cible

◆ Double encapsulation

- Le vlan 10 est enlevé par le 1^{er} switch
 - ◆ Permet d'atteindre via le second switch le vlan 20



Attaque sur une machine

✧ Plusieurs étapes

- ✧ Recherche des ports (services) ouverts
- ✧ Recherche des applicatifs et leur version qui tournent
- ✧ Recherche via les BDs d'exploit si faille présente

- ✧ Une fois, prise en main
 - Mise en place d'une backdoor
 - Utilisation d'un centre Command & Control (C&C)

✧ Protection

- ✧ Limiter le nombre de ports ouverts
- ✧ Mettre à jour les logiciels
- ✧ etc...

Attaque sur un réseau (1)

✦ ARP spoofing

- ◆ Envoies-en continue de trames ARP
- ◆ Facilement détectable sur des switches manageables

✦ IP spoofing

- ◆ Existe, mais très difficile à mettre en place
- ◆ Utiliser pour le DOS

✦ Man in the middle

- ◆ Faire transiter les données via la machine pirate
 - Soit 2 communications distinctes
 - Soit comme routeur (mais impossible d'intercepter conversation chiffrée)

Attaque sur un réseau (2)

✦ DOS ou DDOS

- ✦ objectif : saturation des connexions réseaux d'un PC
 - Ping flooding
 - Attaque smurf (idem, mais icmp en broadcast)
 - Attaque TCP syn
 - Epuisement des connexions TCP
- ✦ Contre-mesure
 - test de la taille des paquets
 - test des adresses source et destination (ainsi que loop-back, unicast, multicast...)
 - test de la fragmentation
 - test du nombre de SYN (contre-attaques TCP)
 - Load-balancing

Attaque sur un réseau (3)

✦ Installation de virus

- ◆ Phishing
- ◆ Via sites webs infectés
- ◆ Via des exécutables, des documents, etc....
- ◆ Faille logicielle

✦ Prise en main via un BotNet

- ◆ Utilisation : DDOS, spam, minage, bruteforcing, ...
- ◆ Raison économique (location de botnet)

Attaque sur le DNS

✦ DNS est encore un protocole en clair

- ◆ Protégé contre DDOS (suite à l'attaque de 2007)
 - Utilisation des adresses anycast
- ◆ Attaque possible sur les caches DNS
 - Empoisonnement du DNS
 - Faire correspondre une fausse @IP à un nom

Utilisation de DNSSec

MITM

✦ Attaque Man in the Middle

- ◆ Plusieurs vecteurs d'attaque possible
- ◆ Objectif : attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de transmission entre elles a été compromis.

Sécurisation d'un réseau

Défense en profondeur

Objectif : Ralentir l'attaquant

Aucun système n'est sûr

- > faille 0-day
- > nouveau virus
- > indiscretion d'une personne,....

- > bug dans un logiciel
 - revue de code
 - test de conformité, de fuzzing,

Sécuriser un réseau

✦ Equipement possible

- ✦ Switch
- ✦ Routeur ???
- ✦ Pare-feu
- ✦ IDS/IPS (TAP : Terminal Access Point)
- ✦ WAF (Web Application Firewall)
- ✦ RASP (Runtime Application Self-Protection)
- ✦ proxy , reverse proxy
- ✦ Serveur VPN, serveur cryptographique

Sécuriser un réseau (2)

✦ Moyen logiciel

- ✦ Durcissement du noyau des serveurs
- ✦ Utilisation d'adresse privée
- ✦ NAT
- ✦ Chiffrement des données
- ✦ VLAN
- ✦ Interdire certains protocoles ou fonctionnalités (DTP, netbios, ttl de icmp,)
- ✦ Antivirus, EDR (Endpoint Detection and Response)
- ✦ Sauvegarde des données