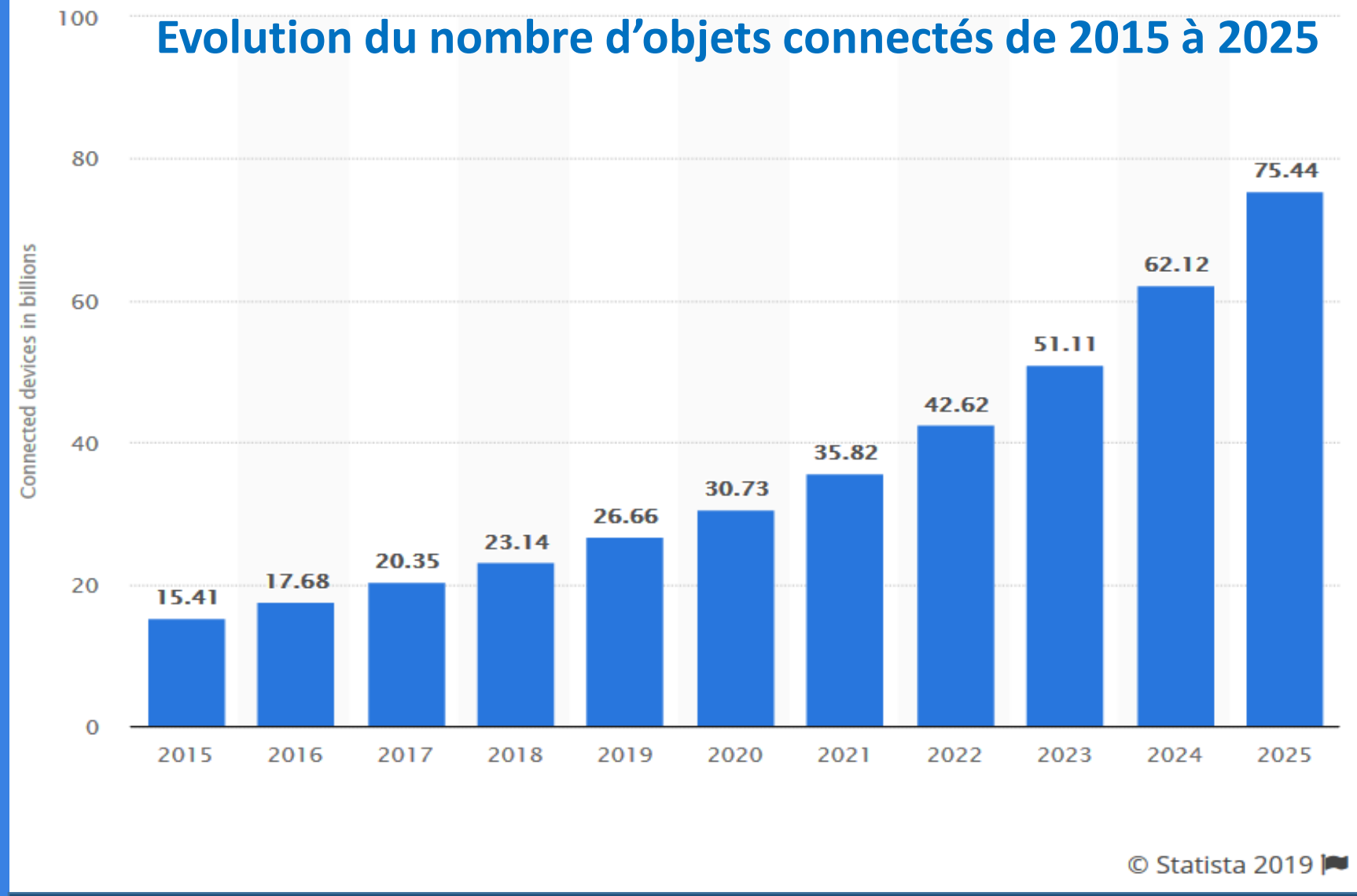
Protection des données à caractère personnel au profit des étudiants

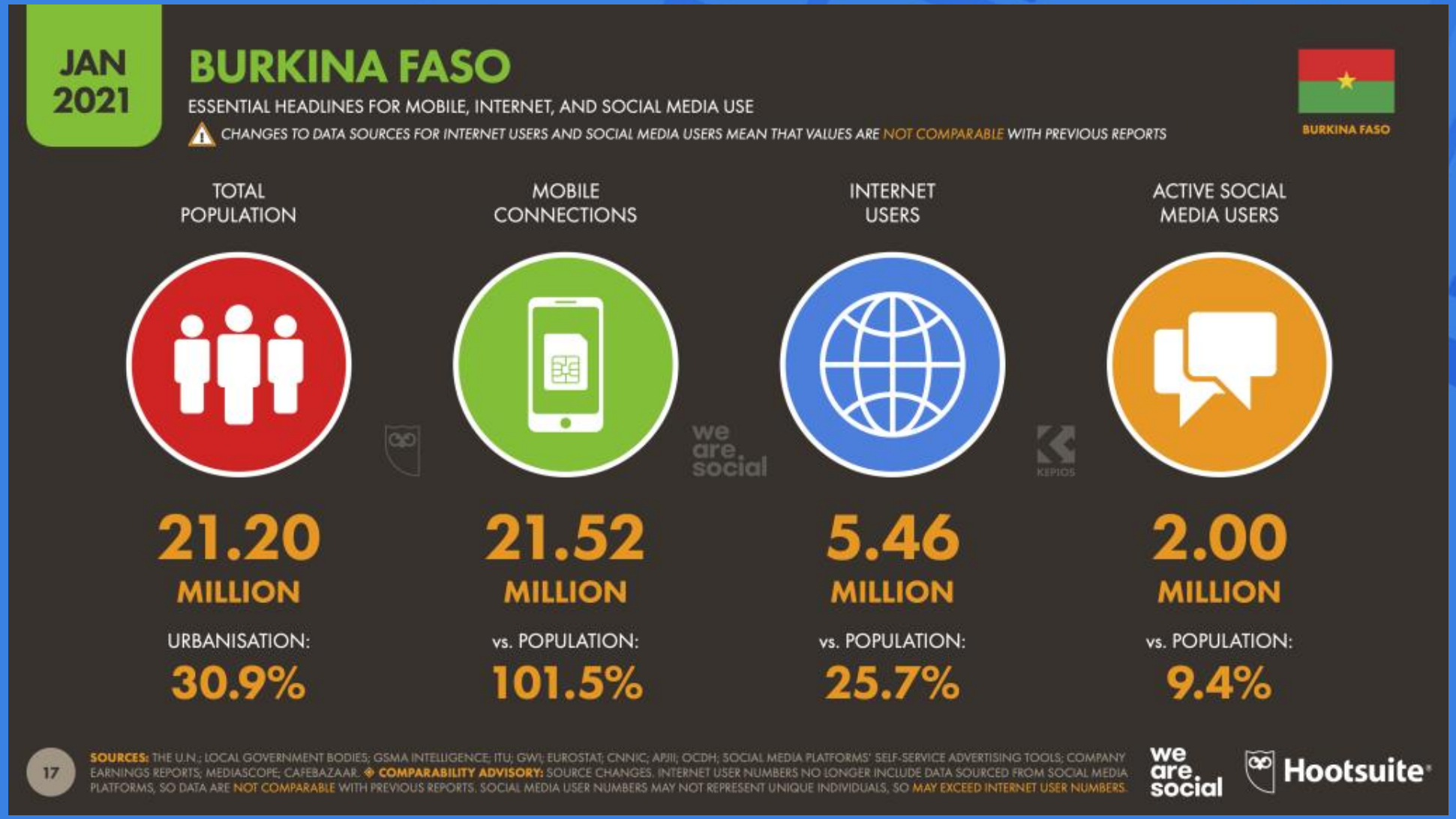
Internet Society

Plan

Introduction



Introduction



Données

- Faits non organisés qui peuvent être transformés en informations significatives
- Se présentent sous forme de Texte, chiffres, symboles, images
- Les gens génèrent des données en permanence
- Nom, numéro de téléphone, photo, sms
- Ces données peuvent vous sembler inutiles mais peuvent être précieuses pour une personne qui planifie une attaque sur vos biens numériques

Données vs Informations

- données traitées sur lesquelles se fondent les décisions et les actions.
- Ce sont des données qui ont été traité sous une forme significative pour le destinateur et qui a une valeur réelle.
- La différence entre les données et les informations est subjective
- la musique vs le bruit

Donnée personnelle

Toute information identifiant directement ou indirectement une personne physique.

Donnée sensible

Informations qui révèlent:

- **l'origine raciale ou ethnique, les opinions politiques,**
- **les convictions religieuses ou philosophiques ou l'appartenance syndicale,**
- **le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique,**
- **des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.**

Règlements

- En 2014, les membres de l'Union africaine (UA) ont adopté la Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel (convention de Malabo)

La Convention de Malabo est divisée en 4 chapitres :

- Chapitre 1 : les transactions électroniques
- Chapitre 2 : la protection des données à caractère personnel
- Chapitre 3 : promotion de la cyber sécurité et lutte contre la cybercriminalité
- Chapitre 4 : dispositions finales

Règlements

- Le règlement général sur la protection des données (RGPD) responsabilise les organismes publics et privés qui traitent les données.
- Vous collectez ou traitez des données personnelles ?
- Adoptez les bons réflexes !

RGPD

RGPD: les 9 principales mesures qui encadrent votre vie numérique

- ❑Un vrai consentement
- ❑Inscription d'un enfant
- ❑Emporter ses données
- ❑Droit à l'effacement

RGPD

les 9 principales mesures qui encadrent votre vie numérique (suite)

- ❑Profilage par algorithme
- ❑Actions de groupe
- ❑Piratage des données
- ❑Point de contact unique
- ❑Grosses amendes

Loi N°010-2004/AN

- loi N° 010-2004/AN portant protection des données à caractère personnel.

- Protéger au Burkina les droits des personnes en matière de traitement de données à caractère personnel, quels qu'en soient la nature, le mode d'exécution ou les responsables

Loi N°010-2004/AN

- loi N° 010-2004/AN portant protection des données à caractère personnel.

- Article 26: une autorité de contrôle dénommée Commission de l'Informatique et des Libertés (CIL).

Elle est chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations et en contrôlant les applications de l'informatique aux traitements des données à caractère personnel.

Loi N°010-2004/AN

Les sanctions, article 46 à l'article 55

- Procéder ou de faire procéder à des traitements automatisés d'informations nominatives
- Communiquer à des tiers non autorisés ou accéder sans autorisation ou de façon illicite aux données
- Collecter des données par un moyen frauduleux, déloyal ou illicite
- Hors les cas prévu par la loi, le fait de mettre en mémoire informatisée, sans l'accord exprès de l'intéressé
- Le fait t'entraver l'action de la commission
- 3mois à 5 ans de prisons et 1 00 000 à 3 000 000 CFA

Règles de protection

Grands principes des règles de protection des données personnelles

- ❑Le principe de finalité
- ❑Le principe de proportionnalité et de pertinence
- ❑Le principe d'une durée de conservation limitée
- ❑Le principe de sécurité et de confidentialité

Nos données personnelles

- ❑ **Elles se baladent de serveur en serveur**
- ❑ **Difficile de supprimer totalement**
  - ✓ **Ex: WhatSapp**
- ❑ **Conserver pendant un temps utile (loi)**

Les plus recherchées 1

LES INFORMATIONS SOCIO DEMOGRAPHIQUES

- ✓ **Nom, âge, sexe, marié ou célibataire, enfant**

Collecter via des formulaires

Les plus recherchées 2

- **LES INFORMATIONS COMPORTEMENTALES**
  - ✓ **Les habitudes d'achats,**
  - ✓ **les sites visités,**
  - ✓ **la durée de session**

- **Elles sont collectées lors des visites sur des sites et sur la base des actions; cliques**

Les plus recherchées 3

- **LES CENTRES D'INTERETS**
  - ✓ **Sport, couleur, politique, voyage**

- **Elles sont collectées lors des visites sur des sites et sur la base des actions; cliques**

Les plus recherchées 4

- **LES DONNEES RELATIVES A LA NAVIGATION**
  - ✓ **Le type d'appareil, la localisation,**
  - ✓ **le numéro du portable ou le numéro IMEI (International mobile equipment identity)**

- **Elles sont collectées lors des visites sur des sites et sur la base des actions; cliques**

Importances

Ces données collectées permettent aux entreprise ou GAFAM de:

- ❑ **Les données sont utilisées pour les statistiques**
- ❑ **L'intelligence artificielle**
- ❑ **Les études de marché**
- ❑ **Les publicités ciblées**
- ❑ **Recrutements dans les entreprises**

Risques

- Un surplus de mail
- Destruction de la réputation
- Non-respect du droit à l'image et à la vie privée
- Usurpation d'identité
- Vol d'argent

Méfiez-vous des hameçonnages

- vise à tromper des personnes à poser certaines actions:
  - ✓ cliquer sur un lien malveillant ou de télécharger et installer des maliciels sur un appareil,
  - ✓ répondre à une demande d'information personnelle à des fins d'extorsion.

- Bonne pratique
  - ✓ Vérifier l'identité des courriel avant l'ouverture
  - ✓ Ne jamais cliquer sur des liens intégrés aux courriel suspects
  - ✓ Ne jamais fournir d'information confidentielle en réponse à un courriel.

Méfiez-vous des hameçonnages

- méthodes d'ingénierie sociale sont conçues pour inciter les utilisateurs à fournir leur information personnelle
  - ✓ hameçonnage par message texte
  - ✓ hameçonnage par message vocal
  - ✓ comptes de réseaux sociaux compromis ou contrôlés par des cybercriminels.

- Ne donner pas fois à tout
  - ✓ Message texte sms
  - ✓ Message vocal
  - ✓ Réseaux sociaux

Sécuriser vos comptes en ligne

- ❑Les comptes en ligne se multiplient à chaque connexion
- ❑Sécuriser vos informations sensible sur des sites

- ❑Assurez-vous de suivre les étapes
  - ✓ Validez la légitimité du site : https, cadenas, certificat
  - ✓ Méfiez-vous du vol d'identité
  - ✓ Utilisez l'authentification multiple si possible

Connexions wifi publiques

- Il est parfois tentant d'utiliser des réseaux wifi ouverts

- Ne fournissez jamais votre adresse, votre information de carte de crédit ou toute autre information personnelle sur un réseau ouvert.

Publications

- position
- Multimédia; audio, image, video

- Ne fournissez jamais votre adresse, votre information de carte de crédit ou toute autre information personnelle sur un réseau ouvert.

Module 2

Plan

- Personal Brading
- Données à caractère personnel, et ingénierie sociale

Personal brading

- Définition

Le personal branding est une pratique qui consiste pour un individu à promouvoir lui même son image et ses compétences par le biais des techniques marketing et publicitaires utilisées habituellement pour promouvoir une marque.

Personal brading

- Comment construire son personnal brading

- soigner votre photo de profil
- soigner votre réputation
- mettre à jour très régulièrement vos profils et différentes actualités

Ingénierie sociale

Définition

L'ingénierie sociale est une technique de manipulation utilisée par les cybercriminels pour inciter les gens à partager des informations confidentielles.

Ingénierie sociale

1. Hameçonnage

L'hameçonnage exploite des tactiques incluant des courriels, des sites Web et des messages textes trompeurs pour voler des informations personnelles et corporatives confidentielles. Le succès des criminels utilisant ces tactiques réside dans le fait qu'ils prennent soin de se dissimuler derrière des courriels et des sites Web qui semblent familiers à la victime visée.

2. Harponnage

Le harponnage est un cybercrime qui utilise les courriels pour mener des attaques ciblées contre des individus et des entreprises. Les criminels mettent en place des tactiques ingénieuses pour recueillir des données personnelles sur leurs cibles pour ensuite envoyer des courriels qui semblent familiers et dignes de confiance.

Ingénierie sociale

3. Appâtage

L'appâtage se base sur le désir humain de récompense. Il s'agit d'un type d'attaque d'ingénierie sociale qui peut survenir en ligne et en personne et qui promet quelque chose à la victime en échange d'une action. Par exemple, brancher une clé USB ou télécharger une pièce jointe en échange d'un accès à vie à des films gratuits. L'ordinateur, et potentiellement le réseau, est ensuite infecté par un logiciel qui peut capturer les données d'accès ou envoyer de faux courriels.

4. Attaque de point d'eau

L'attaque de point d'eau (Water-holing) cible un groupe d'utilisateurs ainsi que les sites Web qu'ils visitent fréquemment. Le cybercriminel explore ces sites Web à la recherche d'une faille de sécurité puis l'infecte avec un maliciel. L'un des membres du groupe ciblé est éventuellement contaminé par le maliciel. Cette technique d'ingénierie sociale est très spécifique et difficile à détecter.