Unités 1 et 2 :

Attaques direct : attaques très concrète a votre mot de passe pour ensuite se connecter de la même façon que nous. Peut être faite en physique
Attaques indirect :utilise la ruse pour piéger. Exemple : courriel piégé
dictionnaire :
permutation :
force brut :
distribuées :
proximités :

Authentification : prouver qu'on est bien celui qu'on prétend
identifier : dire qui on est

authentification → avec un mot de passe

- bon mot de passe ?
- comment le choisir ?
- comment le retenir ?
- comment le garder secret ?
- pourquoi ne pas le réutiliser sur plusieurs sites ?

moyen d'authentification :
- facteur d'authentification
- mot de passe (connaissance) → plus utilisé
- clés / badge (possession)
- empreinte digitale (appartenance)
- autre (signature, geste, localisation)

il est important de ne pas utili

Unité 3 :

Authentification par mdp = 2 défaut : faiblesses des mdp définis + risques de divulgations

Un mot de passe qui apporte un niveau de sécurité suffisant est un mot de passe fort.
Mdp fort = assez complexe pour être difficile à deviner par un attaquant

dans un temps raisonnable à l'aide d'outils automatisés de recherche qui mettent en œuvre les différentes techniques d'attaques tel que les attaques par dictionnaire, permutation, force brut, distribuées ou encore de proximités.

- Faiblesse : Ne protège pas d'attaque tel que le piégeage de post, l' Hameçonnage ainsi que l'intersection réseau ou tout autre technique faisant recours a l'ingénierie sociale.

- A besoin : au minimum d'une longueur de 10 caractères (10 milliards de possibilités pour 10 caractère numériques et 35 milliards pour un jeu de 90 caractères), imprédictible = variétés de caractères minuscules, majuscules, caractères spéciaux, chiffres et ≠ d'un mot du dictionnaire, d'une date d'anniversaire ou de naissance, nom d'un animal de compagnie, etc.

- *Attention* : Il ne suffit pas de remplacer les lettres d'un mot du dictionnaire par des chiffres ou des caractères spéciaux
ex : Ballon → B@ll0n ou encore Artemiss → @rt3mi$$ il s'agit de permutation.
Certains caractères, comme les caractères accentués « é, è, à », etc. de nos claviers français ne sont pas toujours disponibles sur les claviers d'autres pays.

- Mémorisation :
  - ° Question secrète → risques en termes de divulgations
  - ° Définir une phrase → appelé phrase de passe ex : « Lunettes : Crayon : Poste : Chemin », « J'aime la F1 ! Je supporte Ferrari » inconvénients : long a écrire fréquemment
  - ° Phonétique → c'est-à-dire à retenir les sons de chaque syllabe pour fabriquer une phrase facile à retenir ex : 2KDO@nowel (2 cadeaux à noël), ght8CD%€ 7am (J'ai acheté huit cd pour cent euros cet après-midi) inconvénients : se rapproche beaucoup du langage SMS qui est déconseillé d'utiliser
  - ° Conserver les premières lettres → consiste encore à retenir les premières lettres d'une phrase comme une citation, ou encore

° Autre moyen mnémotechnique →	les paroles d'une chanson ex : 1Tvmq2tl@ : Un « tiens » vaut mieux que « tu l'auras »… Un calcul (**op:12*5=60**), Un indicatif (L'indicatif 33 pour la France : **(+33)=Fra!**), etc.

Il est utile de combiner plusieurs de ces méthodes ex :
ght8CD%€ 7am!ctc00l → J'ai acheté huit cd pour cent euros cet après-midi ! C'était cool. = Définir une phrase + Phonétique

<u>Unité 4 :</u>

but de l'authentification, sécurisé l'accès de vos comptes, de vos messageries, appareil électronique ou autre service en ligne

les mots de passes ont leurs limites : compromission, divulgations, risque d'oublie

construire avec soins un mot de passe fort :
- minuscules
- majuscules
- chiffres
- caractères spéciaux

10 caractères

le mot de passe ne doit pas avoir de rapport avec le service utilisé ou avec la vie privée.
Précaution supplémentaire lors de la saisie de mot de passe sur des ordi publiques.

Moyen de changer de mot de passe (opti → forcer le renouvellement du mdp min une fois par mois)

mémoriser le mdp → coffre fort ou point d'authentification unique

règle de sécurité sur logiciel /navigateur : condition général d'utilisation ,

HTTPS, signature, carte d’identité, empreinte