Différents types d’attaque sur internet :

Il existe différents types d’attaques d’informatique que peut subir une personne, une entreprise etc... On peut citer :

Le spam : c’est l’envoi en grande quantité de courriers électroniques sur une messagerie, généralement pour que la victime clique sur un lien frauduleux.

L’hameçonnage : **L'hameçonnage ou phishing en anglais est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles.**

L’usurpation d’identité : L'usurpation d'identité numérique se caractérise par l'utilisation de données personnelles d'une autre personne sans son accord. Les informations utilisées doivent permettre d'identifier la victime. Il peut s'agir de ses nom et prénom, de photos, adresse électronique, mais aussi d’adresses IP.

Virus : Un virus informatique est un programme autonome s’exécutant sans l’accord de l’utilisateur. Ce qui le classe dans la catégorie des programmes malveillants. Certains sont, à première vue inoffensifs pour l’utilisateur, d’autres sont moins discrets.

Risque de sécurité interne : Ils représentent tout les risques encourus en interne dans l’entreprise comme : les e-mails frauduleux, le piratage de données, les erreurs de manipulation, l’espionnage industriel, la perte ou le vol.

Les différents moyens de se protéger des différentes menaces sont :

L’anti-virus sous format logiciel qui permet de protéger la machine passivement sans forcément y intervenir activement.

La formation des utilisateurs : La formation est nécessaire pour les utilisateurs de STA car il est important de connaître la sécurité et l’utilisation de certains logiciels techniques.

Le pare-feu : Permet de protéger un réseau d’entreprise des domaines inconnus, et des sites malveillants. Il est obligatoire d’en avoir un pour sécuriser le réseau.

Le VPN : un tunnel sécurisé qui protège vos données personnelles et peut également être utilisé à domicile pour accéder à ses données et aux données des clients de l’entreprise.

Logiciels protégeant des différentes attaques :

Anti-spam permet d’éviter les spams d’e-mails

Anti-phishing logiciel qui permet d’éviter tous les mails d’hameçonnage

Anti-virus logiciel qui permet de lancer des détections de malwares, virus et les mettre en quarantaine

Former les employés

Cybersécurité (antivirus, VPN, filtre anti-hameçonnage...)

Anti-piratage (Reason Core Security)