====slide_001====

bonjour à toutes et à tous
aujourd'hui nous allons vous présenter
du conférence qui s'intitule cyber sécurité
qui fait quoi comment se protéger

====slide_003====

Tout d'abord, commençons par me présenter.
Personnellement, je suis Guillaume Mulair, je suis d'octeur en informatique en Seigneur
chercheur à l'école des mines de Saint-étienne, et mes dothématiques de recherche et
d'enseignement sont principalement l'intelligence artificielle et la super sécurité.
Et j'ai été recrutée à l'école des mines très récemment puisque l'année dernière,
Philippe Bonne, quand à lui est un géniaire et d'octeur en informatique de l'école
des mines de Saint-étienne, il est très fraîchement à la retraite, et ancienne en Seigneur
chercheur de l'école des mines de Saint-étienne, avec pour thématique principale,
l'intelligence artificielle.

====slide_004====

Donc nous nous sommes présentés, maintenant on va faire quelques petits jeux de questions
réponses pour savoir un petit tir de vous dans la salle, puisque j'imagine que le public
est assez diverses, donc tout d'abord, quels sont vos domaines d'intérêt ? Est-ce
que l'informatique l'on fait partie ? Apparemment, donc pas beaucoup de gens sont informaticiens
dans la salle, donc la salle va être présentation très vulgarisée, donc ne vous inquiétez pas,
vous devriez être capable de comprendre la plupart de ce que je vais dire.
Ensuite, est-ce que vous êtes utilisateur ou utilisatrice d'autinimérique, de type ordinateur,
smartphone, tablette, hériteur, etc ? Oui, alors on voit qu'une grande proportion d'entre
vous l'est, effectivement, aujourd'hui, il y a très très peu de gens qui n'ont pas
au moins un outil numérique à la maison. Ensuite, est-ce que vous avez une petite idée
de si vous utilisez le système d'observation qui s'appelle Windows ou est-ce que c'est
macOS, est-ce que c'est Linux, est-ce que pour le téléphone ou la tablette, est-ce que

c'est plutôt iOS ou Android ? Ok, donc une bonne proportion d'entre vous le sait, mais
j'imagine que c'est quand même là, on commence à rentrer dans les détails un peu techniques,
donc j'imagine que beaucoup d'entre vous ne savent pas non plus de quoi je parle là,
donc c'est juste pour établir un peu qui sait quoi et qu'elle est votre niveau d'informatique
que je pose ces différentes questions. Ensuite, une autre question, parce que nous allons
parler un peu de ce qui est réseau informatique, qui connexion le web, mais aussi les réseaux sociaux.
Est-ce que par niveau, il y a beaucoup d'utilisateurs et de satrices de réseaux comme
Twitter, Facebook, LinkedIn, Instagram, TikTok ? Oui, une grosse partie d'entre vous en
l'air d'être utilisateur de réseaux sociaux, ok, très bien. Et une dernière petite question
assez récemment, qu'est-ce que vous savez de la cyber-sécurité, par exemple, est-ce
que vous avez entendu ? Fait que ce serait, les dernières attaques, failles ou fuits d'informations
ou des problèmes liés à l'informatique, donc vous n'ont rien entendu parler récemment
dans les news, donc il y a différentes outils, effectivement là aujourd'hui, on entend
beaucoup parler liage, je vous entends parler liage, ok, d'accord, bon, de toute façon,
et la petite dernière question, c'est d'essayer de savoir un peu, qu'est-ce que vous
attendez de cette conférence, pour savoir un petit peu, ok, j'imagine que globalement
savoir un peu, voilà, le panorama un peu de tout ce qui existe comme problème aujourd'hui,
surtout ce qui est le plus important, c'est comment est-ce qu'on se protège de tout ça,
c'est bien ça, entre en ce moment, ça va être ce qu'on a prévu de vous dire.

====slide_005-6-7====

On va commencer, je vous ai mis des petits exemples pour essayer d'être un peu un peu
norma de ce qui se passe, de moche en ce moment dans l'informatique.
Là, j'ai mis trois exemples qui date de 2022, je les ai gardés, j'ai réfléchi à
prendre quelques exemples plus récents, mais je les ai gardés parce que je l'ai trouvé
assez intéressant.
Le premier en haut du progrès, c'est l'idée qu'il y a les informations de 147 000
l'ionnée qui sont dans la nature, alors c'est pas forcément les informations par exemple de la
carte manquée, etc. on pense que la fuite vient par exemple d'une mairie ou quelque chose

comme ça, d'un petit chier qu'a refuté, et l'idée c'est que, bon, il y a quand même le nom, le prénom, l'adresse, peut-être le numéro de sécurité sociale, des choses comme ça, donc pas des informations qui a première a priori pour réparer bien grave, mais il faut savoir que rien que ce type d'informations, si on a votre nom votre adresse, on peut vous écrire un message en se faisant passer pour la mairie, en concrétant des choses, et comme ça sera un message qui est personnalisé avec des informations que vous pensez être confidentielle, vous aurez tendance probablement à faire plus confiance à ces messages, donc voilà, c'était ce petit truc que j'ai retenu, c'était notamment parce que c'est local, c'est des lionnées, donc il ne faut pas croire qu'on est protégé parce qu'on est une petite ville locale, et puis en même temps, voilà sur le fait que les informations ne sont pas forcément si on les croit pas grave, ça dépendant les mains de qui elles tombent, en fait.
Ensuite, il y a le petit rigolo qui est au milieu, c'est Amazon, donc je ne sais pas si vous connaissez les Amazon Echo, oui d'accord, donc beaucoup d'entre vous connaissez, donc c'est ces petites boîtes qui, à qui on peut poser des questions et qui nous répondent directement, et bien il faut savoir ce qu'il y a un gars qui pour ça musait à poser la question à son Amazon Echo, est-ce que ma femme me trouve, et il se trouve que la Amazon Echo a répondu oui, et du coup, il a été particulièrement étonné, et quand il a fouillé un peu, il a découvert qu'en fait, on peut accéder aux informations qui sont stockées par le Amazon Echo, et en gardant dedans, il est tombé sur le fait que, en fait, sa femme utilisait la Amazon Echo pour passer des appels à son amant, et donc il y avait des enregistrements des appels de sa femme à son amant sur la pareille, donc voilà, donc je pense que ça a déjà été dit plein de fois dans les news, que ces appareils, ils peuvent agir comme des espions, et ils ont ça beaucoup, même beaucoup plus que nous-mêmes sur nous-mêmes, donc attention à ces petites choses, et le troisième, en haut, celui sur Microsoft, je les gardais, parce que je suis un peu guisée, je vais bien taper sur Microsoft, mais il faut savoir que ces dernières années Microsoft a fait quand même de très très très grosse board d'un point de vue sécurité, et là, le curan, je vous ai gardé cet exemple parce qu'il est assez parlant, c'est l'idée, c'est qu'aujourd'hui, c'est grosse entreprise, notamment Microsoft, elle stocke beaucoup de service dans ce qu'on

appelle le cloud, j'imagine que ça en a entendu parler, mais du coup, elles accueillent
énormément de données, et donc la moindre moment où il y a une petite fuite de données,
c'est des très très grosses quantités de données qui fuient dans la nature, et là,
en l'occurrence, ils ont fait, ça a un ingénieur chez Microsoft, ou un technicien, a fait
une bête petite erreur, il a oublié une configuration d'un serveur, il a oublié
de le protéger, et donc, il a laissé accessible sur toute internet, et notamment ce serveur
contenait en fait la base de données avec tous les clients de Microsoft, et tous les
contrats en cours ou déjà passés avec ces clients, donc ils ont, en fait, ils se
ont tiré une belle d'un pied de la peau du business, puisqu'ils ont donné à tout
leurs concurrents gratuitement la liste de tous les contrats qu'ils avaient, avec tout
leurs partenaires, donc ça peut permettre, maintenant, d'un point de vue business, d'un
des concurrents, de savoir quels sont les montants des contrats que Microsoft passait avec
ces clients, et du coup, va de faire des propositions un peu plus bas, c'est
d'emporter des marchés, donc voilà, la série erreur qui est tant petit pour
Microsoft, c'est juste eux qui ont suiter leur propre données, donc, entre guillemets, on pourrait
penser que c'est pas très grave, mais malheureusement, des fois, c'est pas
leur propre données qui perd aussi les données de leur client, alors après, je vous
ai mis des nus un peu plus récentes, j'en ai mis deux ici, j'ai appelé le
renouveau de l'ancien, alors on peut pas vraiment lire ce que j'ai marqué, mais il n'y a
une qui a assez rigolote, c'est une attaque qui existe à depuis très très longtemps, donc
des gens qui ont mis des micros potentiellement assez longues distances d'un clavier,
mais ils se trouvent qu'en fait, chaque clavier, chaque touche est un tout petit peu
différente de l'autre, mécaniquement, parce qu'elle a été créée dans un appareil
qui est pas parfait, et ils se trouvent que du coup, si on l'enregistre à distance, le
son qu'elle va produire quand on appuie dessus est un petit peu différente de
celle d'à côté, et donc on peut apprendre avec un système d'inténiance
accessible de machine learning, on peut apprendre à reconnaître
chaque une des touches, et donc réuniquent en écoutant un clavier à quelques
maîtres de distance avec un micro, on peut être capable de détecter qu'est-ce
que la personne est en train de taper sur son clavier, et avec les progrès liars
récemment, ce type d'attaque a beaucoup progressé, il fallait revenu à la

mode, et on arrive maintenant avec 95% de réussites à détecter à distance,
donc elle ne capa rien qu'en écoutant avec un micro, de reproduire ce que la
personne a tapé sur son clavier. Ensuite, comme je vous disais, des fois, c'est des
erreurs de conception, ce n'est pas forcément des hackers qui viennent, ce sont les
concepteurs d'éléments qui ont fait une faute, alors l'occurrence, par
exemple, je ne suis pas six ans entendu, parler du kiat challenge, donc apparemment, c'est des
vidéos qui traînent sur TikTok, d'adolescent notamment, qui ont découvert qu'en
fait qu'il y a les constructeurs à l'automobile, ils ont tellement voulu
réduire les coups, que malgré toutes les attques qu'on connaît aujourd'hui sur les
automobiles, et donc tous les constructeurs mettent un minimum de sécurité sur leur
véhicule, qui a, c'est dit, pour réduire les coups, on va pas les mettre, et donc
il y a des vidéos qui montrent sur internet que des adolescents, rien qu'en
connectant un cable USB sur l'automobile, arrive à voler l'automobile.
Ensuite, je vous ai mis trois exemples, comme je vous disais, j'aime bien tapé sur
Microsoft, alors là, je vous ai dit, en 2023, ils ont vraiment fait la
totale, trois très très grosses erreurs, la première, c'est qu'il y a une
pousse de sécurité dans les ordinateurs aujourd'hui, qui en ferment ce qu'on appelle
une clé cryptographique, une clé de sécurité, qui normalement doit justement
être enfermée matériellement dans cette pousse, pour ne jamais sortir, pour qu'on
ne puisse pas décrypter par exemple le disque dure de votre ordinateur, et
Microsoft a fait une grosse erreur de conception, où il y a une instruction qui
permet d'aller demander à la pousse, de donner la clé, et donc du coup si on se
connecte sur la carte mer, donc sur l'intérieur de l'ordinateur, sur les
câbles qui circulent à l'intérieur de l'ordinateur entre le
processeur et cette pousse, on peut récupérer la clé, et du coup,
quelle que soit le disque dure, et quelle que soit la difficulté avec la
clé qu'il a été chiffrée, on va pouvoir le déchiffrer et récupérer les
informations de l'ordinateur, ensuite, voilà, je vous passe les détails, mais
il y a d'autres, pour savoir que ça ne n'est pas mieux pas, les grosses
d'entreprise comme une croissante.

====slide_008====

Voilà, ça c'était les petits exemples, maintenant je vais vous faire un petit slide de résumé
en fait du paysage, en fait, on va dire, en gros, bon ça, je pense que vous l'avez

compris, les hackers, donc ils attaquent des files de sécurité ou ils exploitent des bugs
de conception, et donc du coup, c'est un jeu du chai de la souris, sans arrêt, quelqu'un
va créer un loge d'itiel, un hacker va trouver une file, la file va être corrugée,
une autre file va être trouvée, etc, donc ça évolue sans arrêt, mais ce qu'on peut
remarquer en 2023, une grosse au modo depuis Covid, qu'il y a une très forte
augmentation des attaques, et notamment, si je fais un peu, c'est un peu arbitraire,
ma séparation, mais en gros, jusqu'en 2020, on va dire, les attaques étaient plutôt
de types assez simples, mais elles étaient faites par des outils assez compliqués,
qui étaient écrits par des attaquants qui étaient plutôt solos, on appelle le
hacker qui est un petit jeune assez doué, effectivement, c'était souvent des
adolescents, je vous ai mis la photo là d'un adolescent, qu'il y a 15 ans, on peut-être
pas compte sur la photo, mais qu'il y a 15 ans, à qui je crois que c'était le
FBI, en tout cas, une grosse institution américaine, et les victimes à l'époque,
ça me souhaitait des adolescents un peu en manque de égaux, ce qu'ils les
intéressaient, c'était d'attaquer les trucs les plus flagrant, donc en l'occurrence,
des militaires, parce qu'ils sont censés être très bien protégés, donc si on
arrive à les hacker, ça fait du bien à l'égo, et puis des entreprises, parce
que les entreprises, c'était des grosses entreprises avec de l'argent, et donc
quand le but était d'avoir l'argent, attaquer des grosses entreprises, ça faisait
rentrer plus d'argent, et en fait, depuis, on va dire, on va être de
Villes-Main 2, de 2023, les attaques changent beaucoup, notamment elles sont
beaucoup plus compliquées, en général, elles ont plusieurs étapes, elles ne sont pas
que techniques, notamment, et en général, je vous le p'tit logo, là de
recyclage, c'est pour dire qu'il y a plusieurs étapes, et le petit bonhomme
plus l'ordinateur, c'est pour dire qu'il y a généralement une première phase
humaine, en fait, où on, par exemple, on va appeler la secrétaire pour
récupérer le mot de passe de la secrétaire, puis une fois qu'on a accès à
l'ordinateur de la secrétaire, on va rebondir sur une machine qui est dans le
réseau, puis on va aller sur la machine du directeur, puis ou sur le
la machine du directeur du département informatique, etc.
Donc elles sont de plus en plus compliquées, mais par contre elles utilisent des outils
de plus en plus simples, donc c'est la combineaison de plein d'outils assez

simples, et ces outils simples, en général, comme ils sont simples, ils sont
développés assez rapidement, et souvent les accords, bah ils les partagent sur
Internet, donc du coup, même pour des gens qui n'ont pas beaucoup de connaissances,
c'est assez facile de trouver ces outils et de les employés, même si on sait pas vraiment comment ils fonctionnent. Du coup, en fait, ces attaques, elles
sont très différentes aussi, par le fait que les attaquants sont différents,
normalement, c'est pas si vous l'avez entendu, ou cet acronyme, là, à péter,
Advanced Persistence Fret, c'est ce que le nom qu'on donne, en fait, à ces groupes
de hackers qui sont généralement des groupes très gros, très bien constitués,
généralement supportés par des états, et qui ont beaucoup d'argent, donc potentiellement des grosses machines pour et des grosses puissances de calculs pour
essayer de rentrer dans les machines de leurs cibles, donc très grosses différences par rapport aux hackers, solos, qu'on avait à l'autre, et les victimes,
et depuis quelques années, malheureusement, il n'y a plus vraiment d'étiques, le but
c'est plus vraiment d'attaquer les militaires pour faire ce grossir son ego, c'est
des gens qu'on peut, aucun scrupule, et ils attaquent des ONG, des hôpitaux, des
écoles, il y a beaucoup, comme je vous disais, comme ça, les appétés sont supportés par des états souvent, il y a aussi les attaques envers des autres
faisants politiques pour essayer de récupérer les informations pour pouvoir les
emprisonner ou les choses comme ça, et comme je vous disais, comme ce sont les
attaques qui marchent souvent par rebond, donc on attaque une première personne un
peu inocente, pour rentrer dans le réseau de son entreprise, pour, après, pouvoir attaquer plus globalement l'entreprise, et bien souvent, on attaque aussi
des particuliers un peu inocents, donc voilà, en quoi, les nouvelles tendances
font que vous êtes particulièrement touchées par ces attaques, et par la cybersecurité en général.

====slide_010====

Donc, en ce qui va nous confermer, en tout sortant qu'utilisateur d'informatique, en gros,
j'ai essayé de séparer, il y a deux choses, la première chose, c'est les appareils qu'on
utilise, on va dire, donc qui peuvent être plus ou moins faillibles, notamment on va
voir trois types d'attaques, les attaques physiques sur l'appareil, les attaques sur les mots

de passe et les attaques potentiellement par franchement de périphériques extérieures
pour que les usb et il y a des attaques qui peuvent venir d'autre extérieur quand la
machine est connectée en réseau, alors aujourd'hui quasiment toutes les machines sont
connectées en réseau, mais voilà, elles sont aussi des petits attaques plus spécifiques
au fait qu'elles sont connectées en réseau, notamment les attaques par phishing, par courriel,
ils attaquent par des sites web malicieux, et il y a des plus qui est phishing spam par SMS
qui peut arriver aussi en téléphonie, et puis de plus en plus, on a des objectes
à connecter en réseau sociaux, donc on a des connexions si vers l'extérieur qui peuvent
être sources de cochonerie qui arrivent sur mon achet.

====slide_012====

Alors, regardez la première partie qui est l'accès physique à la machine, donc la machine
sur laquelle je fais la démonstration, je ne vais pas la démonter sinon je peux plus
vous faire les affichés les transparents, mais je vais ramener une petite machine ici
à côté où je peux vous montrer, en fait, si jamais, par exemple, vous êtes employé
dans une entreprise et puis vous quittez le bureau pour aller boire un récaffé avec
les copains et qu'on vous vole votre ordinateur, et après, on n'a pas forcément besoin
de votre mode passe pour s'identifier sur la machine, si on accès physique à la machine
et qu'on peut récupérer le disque dur, donc là, comme je vous montre sur la machine,
je dévisse 3 vis, jour en petit capot, je tire le disque dur, et donc ce petit rectangle
là, de plastique métal, contient en fait toutes les informations de vos photos, vos modes
passe, vos fichiers worth, etc. Donc, on peut les récupérer juste si on a un accès physique
à la machine, d'où l'intérêt de protéger l'accès physique à sa machine, et
il y a une autre façon de le faire, qui est un peu plus discrète, où c'est de redémarrer
votre machine, en brancher une clé USB un peu spéciale, je ne veux pas faire la démonstration
ici, mais l'idée, c'est qu'on peut aussi accéder aux fichiers, de cette manière-là,
un peu plus discrète. Ce que je n'ai pas dit ici, c'est que ça marche bien, c'est
assez simple, si le disque dur n'est pas chiffré, et il se trouve qu'aujourd'hui, heureusement,
la plupart des systèmes d'exploitation, donc Windows, MacOS ou Linux, quand vous installez

votre machine, ou en tout cas, quand vous achetez la machine, et qu'elle est déjà installée,
souvent, soit le disque dur est déjà chiffré, soit il y a une option où vous demandes,
où vous pouvez aller configurer dedans, le chiffre est le disque qui est écrit ici sur
le 30 par an bleu, c'est un lien que vous pouvez cliquer, et ça vous explique comment
chiffrer votre disque dur, s'il ne l'était pas, dès le début, et donc la meilleure protection
c'est de surveiller votre ordinateur, de fermer la porte de votre bureau à clé...

====slide_013====

Ensuite, la deuxième attaque possible c'est à admettant que je vois donc que vous avez
laissé votre bureau ouvert pendant que vous avez de prendre café avec les collègues,
si vous n'avez pas protégé votre ordinateur, je lis vous être connecté dessus, et donc
ce que je peux faire, c'est récupérer des petits fichiers, alors qu'ils s'appellent
système et sames, vous vous émitent tous les détails ici pour reproduire l'attaque pour
montrer que ça se fait en trois étapes, c'est pas très compliqué, mais je ne vais pas
rentrer dans les détails, je vais faire un petit démo, donc là c'est vrai, si je lance le logiciel,
je charge un de ces fichiers système sames, une copie que j'ai faite d'un ordinateur Windows
que j'avais, dans lequel on voit toute une liste ici de mots de passe, en fait,
tout le charabia qu'on voit à droite, c'est le mot de passe qui est entre guillemets chiffré,
et à gauche vous voyez le nom des utilisateurs, donc je peux ciblez un utilisateur en particulier
où tous, et donc si je lance le logiciel, vous voyez le premier mot de passe, passe un
de trois qui a par eu, donc ça m'a de passe très court, donc on le trouve assez facilement,
et vous voyez quelques secondes après, on voit le mot de passe, passe soir d'un de trois,
qui est découvert, donc passe soir d'un de trois, P, A, S, S, W, O, R, D, 1, 2, 3, vous voyez
qu'il y a quand même 11 caractères, donc un mot de passe de 11 caractères, je l'ai cassé,
je l'ai retrouvé en quelques secondes, vous voyez, il faut savoir que souvent vous allez
sur des sites web, par exemple les impôts ou des choses comme ça, et on vous dit il faut
absolument un mot de passe de 8 caractères parce que 8 caractères c'est sécurisé, et bien
c'est plus vrai, on a une telle puissance de calcul aujourd'hui, ça avance tellement

vite au niveau des machines, que aujourd'hui un mot de passe de 11 caractères peut être
cassé en quelques secondes, donc il faut des mot de passe de plus que ça, donc là
ce que je vous disais, les premières solutions, déjà quand vous quittez votre bureau, c'est
de verrouiller votre écran, donc de faire en sorte que le mot de passe il doit être entré
pour pouvoir accéder à vos fichiers, donc je ne peux pas récupérer vos fichiers
systèmes et ça, si vous verriez votre écran, il faut que les mot de passe soit long, donc
aujourd'hui, par exemple à l'école des mines de synthétien, nous devons utiliser plus
de 14 caractères, c'est une politique de l'entreprise, de l'institution, mais voilà
en tout cas aujourd'hui les connus par les organismes d'État qui s'occupe de la
sécurité informatique, recommande plus de 10 caractères dés aujourd'hui, et il y a un
petit exemple que je voudrais vous montrer là, c'est donc une bande dessinée de quelqu'un
qui s'appelle XKCD, qui aime bien faire de la vulgarisation, notamment informatique,
mais assez scientifique, quoi, et voilà, c'est un peu du charabia, mais il fait essayer
de vous expliquer, en gros ce qui montre, c'est que le plus important, c'est pas d'avoir
un mot de passe qui est justement du charabia, avec plein de mélange de caractères
de minuscule, de majuscule, de point d'esclamation, de chiffre, etc, en fait le plus important
c'est que le mot de passe soit long, donc là il fait un peu une démonstration dans
cette BD, en quelques cases, que le plus important, c'est la longueur du mot de passe, donc
une technique qui donne, parce que forcément si on a des mot de passe très long, il
voit d'autres en plus difficiles à retenir, donc la technique qui donne, c'est
dire, vous choisissez aller à toi-même en quatre mots dans le dictionnaire, et vous
les coller, et ça vous fait un mot de passe, alors si vous êtes ambitieux, vous pouvez
aussi essayer de rajouter des lettres, des chiffres, des point d'esclamation, des minuscule,
des majuscule, mais en tout cas, rien que utiliser quatre mots du dictionnaire, en gros,
ça vous fait un mot de passe très long, qui est largement suffisant pour ne pas être cassable
dans quelques secondes aujourd'hui, et après, comme il le disait, voilà, il
fait un petit exemple avec hors stipple, etc, donc cheval à grave, et je ne sais pas quoi,
donc en plus, ça va par quatre mots de la langue, vous pouvez vous imaginer une petite
histoire, ou, enfin voilà, n'importe quoi, une image, en votre tête, qui vous représente

ce mot de passe, et qui donne facile à retenir, donc c'est très long et facile à retenir,
autre chose très, très importante, c'est que ces mot de passe doivent être uniques, parce
que aujourd'hui, quand je vous ai montré les petits chiffres, un peu à l'éatoire, un peu
bizarre, qui sont le mot de passe chiffré, et je vous ai montré qu'on pourrait
le retrouver, une fois que je l'ai retrouvé, l'espèce de petit numéro chiffré, ça
sera toujours équivalent aux mêmes mot de passe, et donc du coup, si quelqu'un publie
sur Internet, il fait l'équivalence entre ce nombre à l'éatoire, cette chaîne de
caractère à l'éatoire, et le mot de passe, et bien, si j'utilise le même mot de passe
sur un autre site, la personne va pouvoir très facilement trouver le mot de passe sur Internet,
le mot de décoder le mot de passe chiffré, sans avoir même à faire tourner un logiciel,
comme je l'ai fait devant vous, donc une autre chose très importante, c'est d'avoir
des mot de passe uniques sur chaque site, et de là, l'idée que, forcément, ça va
être très, très compliqué de retenir des centaines et des centaines de mot de passe
uniques, est très long, donc du coup, ce qu'on vous conseille, ce qui est conseillé
généralement, c'est d'utiliser ce qu'on appelle des estonaires de mot de passe, donc
c'est une espèce de, de, de, de, de, ça peut être, c'est un logiciel, mais qui derrière
va stocker les mot de passe que vous lui donnez dans un fichier, et ce fichier, il est
chiffré, avec un autre mot de passe, qui est un mot de passe maître, on va dire, et qui va
protéger les mot de passe, alors du coup, faut évidemment que ce mot de passe maître soit
très dur et très compliqué à casser, parce que sinon, si on le casse facilement,
après, on a que ça, tous vos autres mot de passe, donc, c'est un peu le maillon de
faible, du coup, et là, je vous ai mis le nom d'un logiciel, qui est un logiciel
libre, qui fonctionne sous Windows, sous Linux et sous macOS, ça peut être qui passe
XC, qui permet de faire ça, et je vous ai mis aussi le site I Have Been Pond, qui est
là, est un site assez intéressant, donc si je clique de sur le lien, là, vous voyez,
j'ai une interface, avec comme un moteur d'orcheche, où on me demande de rentrer une,
mon adresse email, alors, deux bases, normalement, si on vous demande de rentrer votre adresse
email sur internet, il vaut mieux pas trop la rentrer, parce que vous risquez de
recevoir du spam, donc, c'est assez déconseillé, là, on fait un site de confiance,

donc moi, je vous le dis, vous pouvez le faire, la personne qui est derrière ce site web,
c'est un spécialiste de la sécurité, il va pas regarder votre mot de passe, il va
votre email, il va pas vous envoyer des cochonneries, et ce site est très intéressant, en
sens, vous rentrez votre adresse email, et lui, il a tout une base de données, d'à peu
près, tous les piratages qui ont été faits, on pourrait qu'ils sont connus aujourd'hui,
et avec les mot de passe, ce qui aurait été, déjà, cassé, donc, il va vous dire, quand
vous tapez une adresse email, donc là, je vous tape une adresse email, qui est à moi,
je vous montre, c'est écrit "Oh, no, you have been pond", et on peut voir la liste de
toutes les bases de données qui existent, déjà, où le mot de passe associé à cet
adresse email a été décodé, donc, comme moi, je suis au courant, j'ai changé les
mot de passe sur ces sites web, là, et ça m'évitera qu'un cœur puisse pirater mon compte,
et ce qui est très sympa sur ce site, c'est comme vous voyez, là où on entre l'adresse
email, on peut demander aussi de s'enregistrer, de garder l'adresse email, et de nous
prévenir, quand il y aura une prochaine suite de données, dont le site sera au courant,
si jamais mon mot de passe apparaît dedans, de me prévenir tout de suite pour que j'aille
le changer tout de suite, ça, c'est une chose intéressante à faire !

====slide_014====

Ensuite, il y a le cas classique qui vous disait des connexions de l'appareil extérieur
sur l'orbinateur, connexion physique, du coup, imaginons un scénario SCBET, j'ai
trouvé une clue USB dans la rue, sur le parking, ou ici, dans la salle, imaginons
que la fin de la conférence, on s'en va tous, et puis la dernière personne qui
ferme la salle, trouve une clue USB, à votre avis, comment faire pour retrouver
propriétaire ? Voilà, la plupart d'entre vous me disent, je le connecte sur l'ordinateur, je regarde qu'elle fichait, il y a dedans, et probablement il y a un
fiché qui va plus ou moins m'indiquer à qui ça peut être, et bien il ne faut surtout,
surtout, surtout pas faire ça, je vais vous expliquer pourquoi, donc il y a deux types d'appareils
qui sont assez néfastes, pourrais vous abonner des ennuis, si vous faites ça, le
premier, ce qu'on appelle le rebeur de qui, je peux vous montrer à la petite

vidéo, alors ce n'est pas très très explicite, mais en gros, donc c'est un truc qui
ressemble à une clue USB, mais quand on l'ouvre, si vous regardez, là, en fait,
dedans, il y a de quoi connecter une petite carte SD, donc les petites cartes comme
pour les appareils photos, pour stocker les photos, et l'idée, c'est qu'en fait, ce
t'appareil qui ressemble à une carte, à une clue USB, en fait, quand on connecte
à l'ordinateur, il dit pas "coucou", je suis une clue USB, voilà, les fichiers que je
peux te proposer de lire ou d'écrire, en fait, il va dire "coucou", je suis un clavier,
et la personne qui est malveillante, qui a mis la petite carte SD dedans, elle va
amètre des fichiers dans lesquels elle a écrit ce qu'elle veut que le clavier
génère, donc c'est un faux clavier qui va taper, toujours la même chose, et
très rapidement, et donc, en l'occurrence, dans ce que vous voyez dans la vidéo là, on
n'a pas le temps de voir très très vite parce que, mais c'est ralenti quand même, je
crois que là, il tape plus de 1000 caractères à la seconde, on voit des fenêtres qui
souvent, en fait, simule de souris, qui vient cliquer à un endroit, qui lance une
application, qui tape des commandes, et en fait, là, voilà, il est en train de vous montrer
que la commande qui s'est passée, c'est qu'en fait, on a désactivé l'antiverus, et donc
du coup, votre ordinateur est complètement d'une erreur de main, le deuxième pseudo
clé USB, qu'on peut trouver, ce qu'on appelle le USB killer, que vous voyez ici, et les
petits carré marrons qu'on voit dans l'image, en fait, ce sont des condensateurs, donc en
fait, qu'est ce que fait cet appareil, quand vous le branchez sur la clé USB, et bien,
il y a de l'électricité qui passe, par exemple, quand vous rechargez votre téléphone
sur votre ordinateur, il y a forcément du courant qui passe, bah là, c'est
petit capacité, ce petit condensateur, ils vont accumuler le courant, puis l'accumuler,
l'accumuler, l'accumuler, l'accumuler, l'accumuler, et à un moment quand ils sont
chargés, ils relâchent tout dans l'autre sens, et donc ils envoient des milliers de
volts et d'empères, enfin, et quelques centaines d'empères, dans leur ordinateur, et du coup, ça crame tout, dans leur ordinateur, donc là, je peux
vous montrer pas la vidéo, mais il y a des vidéos là, que si vous cliquez sur le
lien, vous verrez qu'en fait, bien, leur ordinateur peut aller même jusqu'à brûler, et à prendre

feu, tellement la quantité d'énergie qui prend d'un seul coup et violent, et en tout
fait, là, pour le coup, leur ordinateur, il est complètement cramé, c'est plus
la peine d'essayer de l'utiliser, il est bon pour la poubelle, et alors là, pour ça, les solutions,
il y en a qu'une seule, c'est la vigilance, donc ne rien brancher, ou ne rien laisser,
qu'il se soit brancher à votre ordinateur, sans, enfin, si c'est pas quelqu'un de
confiance, c'est un appareil de confiance, et il y a une des choses qui existent dans certaines entreprises, alors on peut désactiver le pot, l'épaure USB,
soit, de façon logicielle, mais donc ça ne protège
rapa contre les USB-killer, puisqu'électricité continuera toujours d'arriver dans
le port, soit, de façon matérielle, il y a des entreprises, ou même des services
secrets français ou autres, en général, dans les machines qui sont chez eux, ils
arrachent les ports USB pour éviter que les déconnexions d'appareils USB qui
se fassent dessus.

====slide_015====

comme je vous disais, une grosse part de la sécurité informatique repose sur la
vigilance, donc c'est bien, quand on, même quand on est juste en train de traiter
sur l'ordinateur, de savoir un peu ce qui se passe sur l'ordinateur, alors là
ce que je vais vous donner, c'est des trucs pour les gens qui se sentent un petit peu à l'aise en informatique,
mais il y a des outils, alors là vous pouvez le voir sur l'ordinateur à moi, là haut,
j'ai tout un tas de chiffres et de petits logos qui indique par exemple à combien le CPU,
donc le processeur de l'ordinateur à quel point il en train de fonctionner, donc quand en
général c'est très bas, c'est qu'il n'y a pas beaucoup de logiciels qui tourne, si c'est
très haut, c'est qu'il y a beaucoup de logiciels qui tourne, si je suis en train rien faire sur l'ordinateur avec
d'un coup ça monte tout seul, ça peut être un indicateur qui est un logiciel malvéant que l'en train de
faire quelque chose, à côté j'ai par exemple la mémoire vive, donc c'est la quantité de choses
qui sont actuellement chargées dans mon ordinateur, pareil, si ça bouche, enfin si je fais rien ça
ne devrait pas bouger, donc si d'un coup je le vois bouger ça pourrait m'inquiéter, et puis voilà
tout un tas d'informations, ou aussi tout ce qui passe sur le réseau par exemple ça peut être
intéressant, sous Windows alors moi je ne suis pas sous Windows, mais sous Windows existe aussi des outils,

je vous en ai mis deux exemples ici, et puis si vous cliquez sur les différentes choses en bleu,
ça va vous expliquer comment installer ou activer cet logiciel pour qu'ils sont en permanence,
ils apparaissent sous Windows et vous puissiez suivre un peu ce qui se passe sur votre ordinateur,
une autre chose pour qu'on s'en a la vigilance, c'est, ça est vraiment certainement entendu,
qu'il faut avoir un antivirus sur son ordinateur, alors de bas aujourd'hui Windows vient
avec le Windows Defender qui est un antivirus fourni par Microsoft, souvent les gens disent que
c'est pas suffisant, qu'il faut en installer un autre, donc vous aimez une liste ici, par exemple,
là m'avait Bitdefender, Norton, Avast, Kaperski, et puis il y a des comparatifs, je vous ai mis en dessous,
alors ça change régulièrement, il n'annait sur l'autre, il y en a un qui est excellentideré comme
meilleur que l'autre, je vais pas rentrer dans les détails, juste de petites choses, celui que ça
appelle Kaperski, il est fait par une société qui est russe, donc aujourd'hui vu que la Russie est
en guerre avec beaucoup de pays, vu que c'est une entreprise russe, elle doit respecter ce que le
gouvernement russe lui demande, et il y a des soupçons, comme quoi le gouvernement russe,
pourrait utiliser le logiciel de cette entreprise pour aller espionner les ordinateurs sur lesquels
il est installé, donc il y a beaucoup d'institutions en France où il ne doivent plus installer
ce logiciel, à l'école des mines, c'était le cas, il est utilisé jusqu'à quelques années,
ce logiciel, ce Kaperski antivirus, parce qu'il était considéré comme le meilleur,
qu'aujourd'hui ils ont dû changer, et puis il y en a un autre qui s'appelle Klam avait,
que moi j'aime beaucoup, c'est un logiciel libre, donc on sait exactement comment il fonctionne,
son code source est publique, mais il est peut-être un petit peu de moins bonne qualité,
parce que la plupart des autres vous verrez ce sont des, ce qu'on appelle friwaire,
donc ils fonctionnent gratuitement au début, et puis au bout d'un mois ils vont dire à
maintenant faux pays, et puis c'est assez ennuyeux à désinstaller après, voilà pourquoi
moi je préfère Klam adhé, et ensuite la dernière chose pour être vigilante, c'est comme
je vous disais souvent, les hackers, ils vont exploiter des failles de sécurité, donc des bugs
de conception dans les logiciels qui sont installés sur votre machine, et des logiciels, par exemple
sous Windows, de base, il y en a plein, vous le savez, la calculette, il y a des jeux,
il y a office, il y a tout un tas de choses qui tournent en permanence sous Windows, donc il faut
corriger ces logiciels à chaque fois qu'il y a une faille de sécurité qui est trouvée,

meilleur moyen de le faire, c'est d'accepter les mises à jour de Windows, les Windows update,
alors je sais que malheureusement sous Windows c'est pas très bien fait, il faut démarrer des fois
plusieurs fois la machine, des fois ça prend très longtemps et on peut pas utiliser l'ordinateur,
mais en tout cas c'est une bonne pratique de sécurité, que de maintenir son ordinateur à jour
régulièrement, et de ne surtout pas désactiver les mises à jour.

====slide_018====

Voilà, ensuite, donc là on a parlé de la partie, vraiment accès physique à la machine,
la machine elle-même, maintenant on va parler plutôt des attaques qui viennent à travers le réseau.
La première chose, je pense que vous avez tout, c'était victime de ce qu'on appelle
à vous recevez déjà en tous du spam, pas soit par courrier, soit par SMS, là je vous
ai mis quelques exemples, du coup je vais vous laisser étudier un petit peu, mais dire
qu'est-ce que vous pensez qu'il fait que ce sont des spam ou pas, et pourquoi ?
Donc dans le premier en haut à gauche, ça vous dit que vous n'avez pas payé
quelque chose pour Netflix, alors déjà quand on vous demande de payer quelque
chose, c'est l'ouche, après bon, heureusement on a des factures à payer, enfin heureusement, on a régulièrement des factures à payer, donc ça pourrait ne pas
être l'ouche, si vous n'avez pas la bonne main Netflix, alors là c'est même pas
la peine, c'est tout de suite un problème, et puis si vous regardez l'URL sur
laquelle on vous demande de cliquer pour aller payer, ça s'appelle régulérialisation Netflix
tout collé.com, donc ce n'est pas Netflix, c'est un autre site, régulérialisation Netflix, et voilà,
c'est probablement une attaque, et si vous regardez en haut, le numéro de téléphone 12 avien, 0,643,39,46,1, ce n'est
une nouvelle fois que téléphone n'a particulier, ce n'est pas numéro ce que c'est suffi qu'il d'entreprise, donc ça, ça aussi, ça serait louche.
Sur celui de droite, alors on voit tout de suite, donc ça vient du téléphone Philippe, Philippe, vous a la nous
a donné ces exemples qu'il a reçu, et en fait vous voyez qu'il a un petit logiciel qui, man de
d'ailleurs, qui est intégré dans les dernières versions d'Android, souvent, qui vous prévient quand
des numéros de téléphone sont connus pour être des envoyeurs de spam, donc là, déjà, vous avez
des petits points d'esclamations, qui vous dites qu'il y a une forte chance que ce soit un spam, encore ça,
un numéro de téléphone qui est d'un particulier, qu'il n'y a pas l'air d'être un téléphone

nu entreprise, et si vous regardez dans le message, votre commande a été expédie, veut y cliquer sur, et vous voyez qu'en fait,
là, on voit, il y a des trucs qui ressemblent un peu en gras ou autre, en fait, les caractères sont pas des
caractères européens, on va dire, c'est des caractères siriliques, par exemple, donc il y a des trucs
qui ressemblent à des y grecs, mais qui sont en fait pas des y grecs, et des choses comme ça, donc ça,
c'est typiquement des choses pour essayer de masquer, des url, où on fait ressembler à quelque chose,
qu'une url, par exemple, si je dis, youtube, en fait, comme le y grec de youtube, je peux le remplacer par le
faux y grec, qui est, en fait, le y grec sirilique, et bah, vous croyez, cliquer sur youtube, mais en fait,
vous allez sur autre chose, et puis le dernier, là, Boursorama Bank, c'est quelque chose qui a été
reçu par email, là, voyez que le look de l'imail ressemble beaucoup à celui de Boursorama,
il y a, voilà, il y a un message, etc, mais en fait, si vous regardez l'expéditeur, en haut,
il y a écrit Boursaud, et c'est s'appelle Noriplay@oudou.fr, donc rien à voir avec Boursorama,
donc l'envoyeur de cet email, il n'est pas du tout Boursorama, et donc voilà, c'est encore un spam.

====slide_019====

Alors sur ce slide, donc du coup on va l'idée c'est là où vous a fait un petit test en live, on peut y avoir un site web de test où on vous montre des mails, on vous demande ce que c'est du spam ou pas, est ce que c'est une arnaque ou pas, et vous devez répondre et après on vous donne la vraie réponse et on vous explique pourquoi, donc très intéressant à faire vous-même dans votre coin, mais on ne va pas le faire pour le moment parce que ça prendrait trop de temps.
L'idée c'est que, c'est, voilà les attaques, aujourd'hui vous avez dû entendre parler de chat GPT, donc l'intelligence artificielle qui est créée par le société OpenAI, et bien en fait, aujourd'hui c'est ce système de phishing qu'on détectait jusqu'à maintenant par des fautes d'orthographe, etc.
Avec des logicèques comme chat GPT qui écrit très très très très bien en français, en anglais, en espagnol, presque toutes les langues assez connues, ça va devenir de plus en plus difficile à détecter.
Et je ne sais pas si vous avez entendu parler de ce qu'on appelle l'attaque aux présidents, l'arnaque aux présidents, alors la plupart d'entre vous n'ont pas entendu parler, donc je vais vous expliquer rapidement, en gros l'idée, je vous ai mis un photo d'un président de grosse entreprise française connue,
l'idée de base, c'est dire, voilà, en fait, c'est quelqu'un, le hacker, qui va appeler par exemple la secrétaire du directeur d'une grand entreprise, et lui dire "Aloh, oui je suis le directeur, bla bla bla, en fait je suis coincé au Congo, là, mais je ne sais pas si tu te rappelles, on avait le contrat pour la société tartampion, qu'on devait absolument en signer avant ce soir à 19h, donc je vais t'envoyer le PDF, et il faudrait que tu le signe avant ce soir, et puis que tu me l'auras.

Et il faut savoir que c'est une des rare choses qui est dans le droit international, c'est qu'un contrat, a partir du moment où il est signé, il est valable, légalement.
Donc même si on peut prouver que vous avez été manipulé pour le signer, voilà, vous pouvez faire tous les procès que vous voulez essayer de récupérer ressout, etc, mais en tout cas, le contrat lui-même, il est signé, il est valable.
Et donc du coup, il y a eu des grosses grosses d'arnaques comme ça aux Etats-Unis, où des gens ont essayé de faire virer des grosses somme, je crois que c'était plusieurs millions de dollars, d'entreprises américaines, vers les Philippines, et ce sont les banques, le dernier niveau des banques, le plus profond au moment où l'argent est vraiment versé vers les Philippines, qui se sont dit, tiens, c'est bizarre, c'est virement américain vers les Philippines, on va appeler l'entreprise, et qui on appeler l'entreprise, et l'entreprise, c'est rendu compte qu'elle s'était faire naquée, et voilà, et donc ça c'est une arnaque qui existe déjà,
mais aujourd'hui, avec les systèmes d'intelligence artificielle comme ChatGPT, on est capable de générer des vidéos, à partir d'une photo du président, de générer une vidéo avec la voix du président et l'image du président en train de parler, vous avez dû en parler des Deep Fakes ou des fake news, et bien, on est capable de faire ça, donc on pourrait même aujourd'hui pas juste un coup de téléphone, le hacker, au lieu de faire un coup de téléphone vers la sacrétère, il pourrait carrément organiser une visie aux conférences avec la sacrétère,
et avoir l'apparence du directeur de l'entreprise et la voix du directeur de l'entreprise pour faire sans arnaque, donc ça va être de plus en plus difficile de détecter ce genre d'arnaque,
donc pour résumer, en fait, comment on fait pour se protéger de ces arnaques, alors on a vu tout un tas de choses, notamment pour les emails ou les spam voir dans ce qu'on appelle les entêtes,
donc l'expéditeur, vérifier si on connaît bien d'où ça vient, ou si c'est une adresse bizarre ou quelqu'un qu'on ne connaît pas, tout le fait que si il y a des logiciels attachés, notamment tout ce qu'on appelle des exécutables,
les points exé, les points bas, tous les points vbs, sont des logiciels qui vont faire exécuter du code sur votre machine,
donc c'est potentiellement du code Malveillon, donc ne jamais cliquer sur des fichiers qui ont cette extension,
il y a ce qu'on appelle les piéchoines classiques, donc les fichiers PDF, les fichiers d'ocque, donc Word ou Excel ou Powerpoint,
donc attention malheureusement, par exemple les documents Word, on pense que c'est juste du texte, mais en fait, c'est pas vrai,
on peut exécuter du code à l'intérieur d'un document Word, et donc du coup, ou d'un fichier Excel, et donc du coup, il ne faut pas cliquer sur, ne pas ouvrir ces fichiers là, si on n'est pas sûr, de l'émette, et du contenu, ensuite on la vu, donc si il y a des liens,
des adresses email ou on vous demande de cliquer ou on vous demande de contacter, et bien ne pas le faire,
autre chose importante, c'est à partir du moment, si on vous dit "Ah c'est hyper urgent, faut faire quelque chose très vite",
et grossissé votre pénis ou des trucs comme ça, tout ce qui est un peu urgent ou actu, trop beau pour être vrai,
il faut vraiment tout de suite rejeter, et alors une des choses, donc pour l'urgence, la meilleure moyen de réagir,
c'est de ne surtout pas réagir tout de suite, c'est de se poser un peu, discuter avec des gens, réfléchir,

parce que justement cette notion deurgence, quand on pousse les gens à réagir rapidement,
en fait, ils débrancheent leur cerveau, faire en say, et c'est connu, c'est les techniques de manipulation connu,
on sait que le cerveau se débranche, et du coup passe en mode, fait n'importe quoi,
d'ailleurs, il y a un très très bon livre qui s'appelle "Technique de manipulation à l'usage des honnêtes gens",
que je vous conseille de lire sur cette technique, qui existe d'ailleurs, et qui sont utilisés dans la vente aujourd'hui,
et que les accueurs utilisent bien l'environnement, et autre chose, donc une technique très importante
que j'ai mis en gras en haut à droite, si vous avez un doute sur un mail ou un SMS,
vous en voient quelque chose, et potentiellement, vous êtes client de Netflix,
et on vous dit, faut absolument payer une facture en retard, et bien, le meilleur moyen de savoir si c'est vrai ou pas,
c'est de contacter l'entreprise qui prétend envoyer ce email, par exemple Netflix, mais par un autre moyen,
donc si on vous en voyait un SMS, on vous dit, il faut payer quelque chose très vite,
utilisez votre téléphone, et appelez Netflix, ou connectez-vous sur internet sur votre compte Netflix,
et allez vérifier si effectivement, il y a une facture ou quelque chose comme ça,
donc ce qu'on appelle utiliser un deuxième canal, si on vous contacte par téléphone, verifiez par SMS ou sur le site web,
si on vous contacte par SMS, verifiez par téléphone ou sur le site web, etc.
Et pour tous ces Arnac, il y a des conseils sur le site du gouvernement sur cybermalveillance.gov.fr,
je vous ai mis un lien ici sur des types de bases, un peu de ce que j'ai mis là,
il y a aussi, il y avait des sites, comme Oaks Killer,
qui vous vous coquiez coller le contenu d'un email, et ça vous disait si c'était une Arnac connue,
alors malheureusement les Arnac, elles évoluent tellement vite que ces sites ont du mal à suivre,
mais ça peut toujours valoir le coup d'essayer, si vous avez vraiment pas d'ami qui s'y connaissent en informatique,
ou si vous avez un gros doute, vous pouvez toujours essayer de mettre votre email dans un système comme ça,
pour vérifier si c'est une Arnac connue.
Ensuite, si vous recevez un courriel ou un SMS malveillant,
le gouvernement a mis un place quelque chose qui s'appelle Signal Spam,
donc qui peut se faire par SMS ou sur un site web pour signaler des messages qui seraient malveillants,
alors malheureusement, c'est mis en place par le gouvernement,
mais sur certains opérateurs, c'est payant,
quand vous, en fait, il faut transférer un SMS que vous avez reçu vers un numéro spécial,
et sur certains opérateurs, envoyez un SMS à ce numéro spécial, c'est payant,
donc ça donne pas très envie d'aider le gouvernement à détecter les Spams, c'est un peu dommage.
Et enfin, un dernier truc très intéressant que les gens ne connaissent pas forcément,

mais qui commencent à être intégrés, par exemple, dans Firefox,
c'est ce qu'on appelle les alias, c'est, en fait,
quand on vous demande votre address email quelque part,
pour recevoir une liste diffusion ou quelque chose comme ça,
bah, au lieu de donner votre vraie address email,
par exemple, disons que ce soit pour moi guillomulaire@gmail.com,
alors attention, c'est pas ma vraie address email,
il n'y écrit rien, parce que c'est quelqu'un d'autre qui va recevoir,
mais en tout cas, au lieu de donner ça, je peux donner une address email,
donc une alias, donc une autre address email,
par exemple, moi, j'utilise un site web qui s'appelle Eriné.imail,
donc du coup, je peux créer un alias, donc je peux créer,
je ne sais pas quoi, guillomulaire@eriné.imail,
et ce site web, en fait, va servir d'intermédia,
donc il va recevoir les messages pour moi,
et il est transféré à mon vrai address email,
donc quand tout va bien, c'est très bien, je reçois mes emails,
comme si de rien n'était,
par contre, le jour où je commence à recevoir des Spams
et que j'y identifie qu'ils viennent de là,
et je peux me connecter sur le site web de Eriné.imail,
et aller désactiver le lien,
donc du coup, le site web des Eriné.imail va recevoir les emails pour moi,
et puis va répondre qu'en fait,
l'adresse email n'existe pas,
et moi, sur ma vraie address email,
je ne receverai jamais, plus jamais les emails de Spams,
et donc ça, je vous le disais, c'est intégré aussi,
en fait, en fait, donc maintenant,
quand on vous demande un site email,
quand on va l'adresser sur un site web,
des fois, ils vous proposent de rajouter un alias.

====slide_021-22====

Une autre chose, c'est les sites web sur lesquels on se connecte régulièrement,
donc là je vous ai mis un exemple typique, je suis connecté, beaucoup de gens sont
connectés à leur adresse email personnelle pendant qu'ils sont au travail, et si sortes
du bureau, comme vous vous disais, tout à l'heure sans dérouiller leurs écrans, moi je
peux arriver, voir sur leurs écrans comme cela, j'ai maille connectée, déjà je peux
lire leurs émails, c'est pas terrible, mais surtout ce que je peux faire, c'est me
déconnecter, arriver sur la page de l'eau guine ici, et si les gens, comme la plus
par des gens le font, ont stocké leur mode passe dans leur navigateur, et bah du
coup je vais voir cette page ici où il y a l'adresse email et puis le mode passe, et

si je clique sur la fixation de mode passe, je vois le mode passe, je peux prendre une
photo, et vite recliquez sur se loguer, et donc on revient à la page qui était
affichée initialement, avec la liste des émails, de la personne, donc en quelques secondes, je désidentifie la personne, je clique sur le bouton affiché
l'imail, tu as affiché le mode passe, je prends une photo, et je réidentifie la
personne, ça ne me prend quelques secondes, pendant que la personne n'est pas dans
son bureau, et j'ai son mode passe pour ces émails, et comme les gens réutilisent beaucoup les modes passe, potentiellement, c'est aussi son mode passe pour ces
réseaux sociaux, c'est aussi son mode passe pour aller acheter sur Amazon, ou des choses
comme ça, donc attention à ça, et juste pour souligner, il se trouve que en
fait, il y a beaucoup de citoyens où on peut faire afficher le mode passe avec un
petit bouton où on peut cliquer, il y a des citoyens où c'est pas possible,
mais ça ne veut pas dire qu'en fait que je ne peux pas avoir le mode passe, je
vous aime une petite démo ici, en fait la façon dont on s'en fait les situeils,
de toute façon, ils ont besoin de tapier le mode passe dans le champ passeware, le mode passe, il affiche les petites étoiles, mais en fait, lui, il
a vraiment le mode passe qui est tapé derrière, et il existe une type technique assez simple, de dire en fait que le champ de texte où j'ai tapé le
mode passe, au lieu d'être un champ de mode passe, où il faut afficher les étoiles à la
passe des caractères, je lui dis l'interprété comme l'adresse mail qui est
au-dessus, comme un champ de texte, bête-à, bêtement, et du coup, il m'affiche le mode passe.
Donc, les solutions, toujours les mêmes, verrouillés son écran quand on quitte son
ordinateur, le top du top, c'est de ne jamais registrer ses modes passe dans
son navigateur, de ne pas configurer le remplissage automatique, et donc la solution,
parce que évidemment, vous allez me dire oui, mais je veux pas même amuser à taper mon logging et mon mode passe à chaque fois que je vais sur un
site web, donc la solution, c'est d'utiliser, comme je vous disais, de tout à l'heure, un
gestionnaire de mode passe qui va stocker mon mode passe, et la plupart des logiciels
qui font les gestionnaires de mode passe sont capables, si vous cliquez sur un
bouton, d'envoyer le mode passe, le l'identifier, donc l'adresse mail et le mode
passe à votre navigateur, pour se connecter, donc vous avez à peu près la même

fonctionnalité, mais les modes passe sont stockés dans un autre logiciel, donc le
site web, quand vous valider sur un site web, n'a pas accès aux logiciels qui
de tourne sur votre ordinateur et donc ne pourra pas récupérer les mots de passe.

====slide_024====

Enfin pour ce qui concerne les réseaux sociaux, il y a une petite vidéo très rigolote
là que je vous ai mises qui s'appelle le Foguru, donc je vais la résumer pour ce qui
ne serait pas en face avec nous, en gros l'idée, c'est qu'il y a des chercheurs qui
sont amusés à faire une petite expérience, donc ils se sont mis quelque part dans la rue
au PIBA, et puis ils ont fait une fausse enquête en disant aux gens bon bonjour monsieur
que je m'allais, ils ont fait une enquête sur l'IRATEP par exemple, donc voilà blablabla
et à la fin ils demandent le nom de la personne, et peut-être son âge, ou je l'en sais rien,
ou quelque chose comme ça, ou son à la récimée, j'en sais rien, mais enfin le type d'information
que les gens donnent sans aucun souci dans la rue pour désenquer, et un peu plus loin,
en fait, il y a une espèce de yurte avec un soi-disant Gourou, et donc le Gourou
invite évidemment les mêmes personnes à rentrer, et ils leur prétendent qu'ils
va leur faire une lecture de l'avenir ou leur dire plein de choses sur eux-mêmes, et
ce qui est très rigolo, donc au fur et à mesure de la vidéo, on voit le Gourou qui
dit à une Nana, qu'elle a un tatouage à tel endroit sur son dos, et il s'avère
que c'est vrai, qu'à une autre Nana, elle a dépensé 200 euros de chaussures la semaine
dernière, etc, jusqu'à un moment où, oui, dit carrément, le numéro de la carte bancaire
d'une autre personne, et donc les gens sont plus en plus étonnés, et au bout d'un moment,
le gars révèle l'astuce, et en fait, il y a un rideau qui tombe, et on voit que derrière
lui, en fait, il y a 85 personnes, entre guillemets, aqueurs, donc des gens avec des cagoules
noirs, sur des ordinateurs qui tapent à toute vitesse, et en fait, ils sont juste connectés
aux réseaux sociaux de la personne, comme la personne, 5 minutes avant dans la rue, pendant
l'enquête, elle a donné son nom et son adresse email, les gens sont simplement allés
sur les réseaux sociaux, voir les publications de cette personne, et comme vous voyez, en fait,

tout ça, c'était des informations qui sont publiquement disponibles, ce sont les gens
qui eux-mêmes, les ennemis sur les réseaux sociaux, donc vous voyez que les gens, quand
vous leur montrent, quand on leur dit, quand vous connaissez leur numéro de carte bancaire,
ils sont choqués, mais en fait, c'est eux-mêmes qui le mettent sur des réseaux sociaux,
donc c'est quand même complètement dingue, il faut faire très très attention à ce qu'on
met, soit même, sur les réseaux sociaux, alors voilà, j'ai mis les grands principes, en
gros, de dire, la plupart des gens vont dire oui, mais ces informations bénignes, j'ai
rien à me reprocher, en fait, le problème, c'est pas que vous pensez que cette information
est bénign, c'est pareil, par exemple, pour votre nom et votre prénom, la plupart des
gens vont les donner un importe qui, dans la rue, rien que ça, si je connais votre
nom, votre prénom, votre adresse, et je peux faire ce qu'on appelle de l'impersonification,
donc vous me faire passer pour vous, auprès, je ne sais pas, de la sécurité sociale,
ou n'importe quoi, donc attention, que ce n'est pas vous qui décidez si l'information
est bénign ou pas, c'est la personne qui reçoit l'information, pour qui ça peut
être intéressant, il y a d'autres types d'informations, voilà, des exemples, moi,
j'avais une d'autres exemples, voilà, avec des amis, une fois une fille qui me demande,
puisque j'étais en service informatique d'une entreprise, avec ce que tu pourrais
acheter mon compte mail, alors je l'avais dit, oui, pourquoi pas, en tout cas, j'ai
la position en tant que informaticien et à tel endroit d'accéder à des machines qui
me permettraient d'intercepter le trafic, etc, mais je ne veux pas spécialement envie de le
faire, et puis, je laisse couler parce que ça me intéresse pas, mais bon, j'avais
tapé sur Google, son nom, juste comme ça, pour voir pour rigoler, alors à l'époque,
ça ne se faisait pas, aujourd'hui, ça s'appelle, typiquement, tapé le nom de
quelqu'un sur Google, pour avoir des informations sur lui, ça s'appelle Stalker, en
anglais, et donc, c'est un truc assez classique que tout le monde fait, mais bon, à l'époque,
ça ne se faisait pas trop, et puis, je suis plusieurs mois après, elle me revient, puis
en prenant le café, elle me dit, bah alors, tu l'as eu, mais on ne voit pas, c'est
tout, et je lui dis, non, mais bon, trouver un, enfin, visiblement, t'as pas eu
le succès à trouver un appartement au Canada, et là, elle est venue toute blanche, et

du coup, on a discuté, c'était rare, heureusement, c'était une amie, et elle m'a
expliqué qu'en fait, bah, il y avait une histoire personnelle, qu'elle devait
partir s'installer au Canada avec son mari, et puis, voilà, mener une vie définitivement
installée au Canada avec son mari, et qu'en fait, ils n'auront plus, juste au
moment, de partir, donc, lui est parti, mais elle est restée en France, et donc, pour
elle, le fait d'avoir un appartement, d'avoir cherché, un appartement, donc, moi,
ce que j'avais trouvé, c'était juste un message, un forum, elle cherchait une
collocation au Canada, donc, pour moi, ça avait aucun sens, mais pour elle, c'était
une information extrêmement importante, et qui révélé beaucoup d'autres choses
sur elle, donc voilà, pour moi, juste pour dire que c'est pas forcément vous, qui
décidait si l'information a de l'importance ou pas, et ensuite, ça dépend de
quand aussi, parce que ça évolue dans le temps, alors là, je vais gagner mon point
Godwin, le point, voilà, quand il dit que très rapidement, quand on a une discussion sur
Internet, on finit par parler des nazis, bah, c'est un peu ça, c'est que, bah, portez
une étoile jaune, aujourd'hui, où il y a 150 ans, c'était peut-être pas très grave,
par contre, il y a une époque, entre 39 et 45, où avoir une étoile jaune, c'était
particulièrement grave, et là, on commence à vivre la même chose aux Etats-Unis, où
il y a plein de jeunes femmes qui cherchaient des informations, qui discutaient
avec des copines sur les réseaux sociaux à propos d'avortement, et maintenant que
l'avortement est interdit aux Etats-Unis, il y a des entités catholiques
extrémistes qui payent des gens toute la journée pour parcourir les réseaux
sociaux, pour retrouver des traces de filles qui auraient parlé d'avortements sur
Internet, pour les accuser, et les amener jusqu'à des procès, parce qu'elles
auraient violé la loi, donc attention, c'est pas parce que, aujourd'hui, ce que
vous avez révélé sur Internet, n'est pas grave, que, dans dix ans, ça ne sera pas grave,
et puis, autre chose qui est très différente par rapport à les choses que
on avait, plutôt l'habitude, enfin, nous, je vais dire, moi et vous, les un
peu plus anciens, bah, c'est que, juste comme maintenant, quand on révélé une
information, on l'a révélé un copain, et puis, au pire, voilà, on était la
risée de tout un groupe social, parce qu'on avait dit une bétise, mais maintenant,

c'est beaucoup plus grave que ça, parce que le numérique, c'est déjà, c'est public,
ça a un beaucoup plus de gens, mais surtout, ça ne s'efface jamais, donc, comme
c'est copier un peu partout, et que c'est dupliqué un peu partout, et que c'est
facile, ça coûte rien dupliqué, bah, même si vous demandez à Google des facées une trace de quelque chose, c'est vous, bah, peut-être que le moteur d'or
cherche Bing et le Microsoft, lui, à une copie du truc, et en fait, c'est une course
perdue d'avance, ce que d'essayer de faire effacer quelque chose, donc, il vaut mieux
ne jamais rien mettre sur Internet, que de le mettre et d'essayer de les facer plus tard, donc, voilà, les solutions, faire très, très, très attention à ce qu'on met sur les réseaux sociaux, parce que, c'est plus ou
moins en gros, peut considérer que c'est public, attention aux informations
qu'on donne aux inconnules, comme l'histoire de donner juste son nom, son prénom, dans la rue, bah, ça peut amener à des trucs assez graves, puisqu'on
peut retrouver votre réseau social à partir de ça, et à partir de votre réseau social, à ceci à l'avoir d'autres informations, et pour informations, voilà, il faut savoir que des entreprises, par exemple, comme
TikTok, il y a eu beaucoup d'histoires, parce que TikTok est une entreprise chinoise, les chinois ont pas de grand-chose à faire des réglementations européennes, et donc, il a déjà été révélé
plusieurs fois que, notamment TikTok, mais c'est vrai avec beaucoup d'autres
applications, qu'elle fuite énormément de données vers la chine.

====slide_026====

On arrive à la conclusion, l'idée, c'est que la sécurité, je pense à voir vous faire comprendre
que c'est un équilibre à trouver entre la facilité d'utilisation et le niveau de risque,
donc je suis typiquement l'exemple des mots de passe, si vous prenez un mot de passe
de 3 caractère, 1, 2, 3, ça va être très facile de le taper dans la porte qu'elle
s'y poêve, surtout si vous utilisez même partout, par contre vous exposez à énormément
de risque, parce qu'il va être très facile à trouver, et si vous utilisez partout, vous
prépirez à la fois votre compte à ma zone, votre compte Netflix, votre adresse mail, etc.
Donc, voilà, il faut les recommandations, c'est donc d'utiliser des mots de passe
de plus de 10 caractères et différents sur chaque site web, donc à chaque fois qu'on
veut sécuriser un peu plus, ça ne nous facilite pas la vie dans notre côté, mais

donc c'est un équilibre à trouver, donc à vous de voir en fonction de ce que vous
cherchez à protéger, quelle protection vous mettez en face.

====slide_027====

Et je vous ai mis pour terminer les 12 recommandations de l'empsie, donc l'empsie, c'est
la section du gouvernement qui s'occupe de la sécurité des systèmes d'information,
et donc ils ont mis des recommandations sur comment se comporter globalement face au numérique.
Globalement, on l'a dit, choisir des mots de passe et qui soient différents, difficiles
et qu'on ne s'assure de pas les stocker n'importe où n'importe comment pour qu'ils
soient, enfin voilà, on les donne pas n'importe qui pour qu'ils soient restes confinantielles,
séparer les usages professionnelles et personnelles, adapter les moyens selon les données
à protéger, c'est ce que je viens de vous expliquer, penser à sécuriser les supports
à MoVib, donc voilà ce que je vous disais, par exemple, vous pouvez aussi, je ne les
pas penser à dire tout à l'heure, mais sur les téléphones portables, aujourd'hui,
il y a souvent une option, il faut aller la chercher un peu dans la configuration,
mais vous pouvez chiffrer le support de votre téléphone portable, et donc du coup,
si on vous vole votre téléphone, on ne pourra pas en le connectant à un ordinateur,
on va dire le contenu. Ensuite, par la messagerie, donc pareil, on a vu les histoires de
phishing, de spam, nous faire attention à d'où vient le mail, ne pas ouvrir n'importe
quel pied s'attacher, etc. Donc, je n'ai pas parlé du comptes administrateur, mais voilà,
faire attention que sous Windows, c'est très facile, en fait, quand vous êtes utilisateurs,
vous installez à logiciel, le logiciel des fois, il vous demande, est-ce que je peux
installer telle ou telle truc sous Windows, malheureusement, il suffit de dire oui, et ça
le fait, donc c'est pas très cotégé, donc faire attention quand on vous demande, quand
l'ordinateur vous dit, attention, sur logiciel, est en train de faire des choses en tant
qu'administrateur, la plupart du temps, il faut dire non, être vigilant, y avoir les
bons réflexes, notamment quand on veut payer en ligne, ça, c'est effectivement, si vous
voulez pas vous faire détourner plein d'argent, peut-être très attention qu'on vous accéde

à vos systèmes de banque, notamment par exemple, essayer d'éviter de le faire sur les
ordinateurs d'autres personnes, dont des cybercafées, donc utiliser plutôt une application
dans votre téléphone portable, ou sur votre ordinateur, penser à faire des sauvequaires
régulaires, ça se paraît, j'ai oublié d'en parler, c'est très important, c'est que du
coup, si par exemple, vous faites attaquer votre ordinateur avec un virus qui est face
tout le disque dure, et bah du coup, si tout était dans votre ordinateur, vous avez
tout perdu, donc penser à acheter un disque dure, par exemple, external, dans
qu'elle vous régulièrement mettez des sauvegates, comme ça vous me perberait que les choses
que vous avez modifiées depuis la dernière sauvegate, donc ça limite la casse en pleine
problème, ensuite, je vous l'ai dit, mettez à jour les logiciels, le système d'exploitation
est installé à un antivirus, pour se protéger au maximum de toutes les nouvelles
files qu'il aurait pu être trouvées, j'en ai pas parlé, mais quand on télécharge des
logiciels, donc c'est pareil, en de la même façon que quand quelqu'un vous envoie
par main l'un logiciel installé, on ne l'intestale pas si on ne sait pas que c'est
une source fiable, de la même façon, quand vous allez sur Internet, n'installez pas
n'importe quel logiciel, vous allez télécharger un tombe, par exemple, si vous voulez installer
la suite Office, allez télécharger sur le site de Microsoft, puisque c'est un produit
Microsoft et installé là, depuis les logiciels, les sources de Microsoft, et puis, donc là,
c'est un truc pour ne pas parler non plus, mais ça reste lié avec les mots de passe,
quand vous avez un réseau wifi, en général, quand vous achetez une connexion
Internet, vous installez une box avec un mot de passe wifi, en général maintenant, il
est assez sécurisé, il n'est pas que ça ne l'était pas, mais l'idée c'est que,
normalement, ce mot de passe, il est écrit sur la box, donc le top du top, c'est
pas garder le mot de passe par défaut, c'est de le changer, pour en mettre un qui n'est
pas celui qui est écrit sur la box

====slide_029====

voilà, je vous remercie beaucoup pour votre
attention, et si vous avez des questions ou des remarques, n'hésitez pas.