L’identité numérique et l’e-réputation sont ce qui nous identifie sur Internet, tout comme dans la vraie vie, il est très simple d’identifier une personne par son apparence et par ce qu’elle fait et ce qu’elle a fait. Il est extrêmement simple de reconnaître une personne par les grandes choses qu’elles ont faites tout comme par ses scandales. Cette image de nous dans le monde numérique est aussi fragile que celle dans la vraie vie, car elle est unique et est extrêmement dure de la réparer. Il nous a été montré récemment, que grâce à nos informations sur Internet, il est possible de prédire les actions futures d’une personne grâce à des intelligences artificielles, grâce à un clone de soi-même sur des serveurs. De plus, ayant déjà fait de la cybersécurité dans mon passé, j’ai acquis des automatismes qui me permettent de limiter le nombre de traces de mon activité.

Pour commencer, je limite au maximum mon activité publique sur les réseaux sociaux. Je pense que la vie privée ne devrait pas être publiée sur les réseaux sociaux, car il s’agit du domaine du privé. D’après moi, dès qu’on commence à communiquer des informations sur soi-même sur Internet, on crée une propre vulnérabilité sur son environnement numérique et social. Par exemple. Je limite le nombre de photo pour faire face à l’OSINT très utilisé de nos jours qui est un renseignement de sources ouvertes ou le renseignement d'origine sources ouvertes, est un renseignement obtenu par une source d'information publique selon Wikipédia. Pour limiter les métadonnées que je transmets sur les réseaux sociaux, j’aime bien utiliser le logiciel Metadata++ qui est un logiciel gratuit et très puissant pour supprimer ou modifier les informations d’une image ou d’un fichier divers.

Pour limiter mon activité sur Internet, je fais office de VPN pour faire face aux cybercriminels par exemple bien qu'inutile face au service du gouvernement. Malheureusement, on nous a privé que les VPN qui sont fournis par des grosses entreprises telles que NordVPN sont des services qui ne marche par et donc qu’il est bien facile de retrouver la vraie identité de l’utilisateur ou encore si on se trouve dans un réseau local les identifiants et mots de passe sur les sites auxquels on se connecte lorsqu’on est connecté sur le réseau. Lorsque j’ai intégré l’armée, on nous apprend dès la première minute ce qu’est l’anonymat dans la vie de militaire, à commencer par ne pas nous appeler par nos prénoms, mais uniquement le nom. Ceci permet de limiter la fuite de nos informations personnelles et à ne pas s’étendre sur notre vie privée. Aucune photo prise à l’armée ne peut être publiée sur Internet sous peine d’une forte amende voire la prison, car cela pourrait mettre en danger les collègues, mais aussi leurs familles.

Une variante de ce système est l’utilisation du moteur de recherche Tor (Celui-ci a la particularité d’avoir accès au réseau en .onion). Ce service est très utilisé dans les pays où les droits d'Internet sont très limités et où l’accès à l’information y est quasiment impossible. Celui-ci est très utilisé par les journalistes tout comme les services de renseignement ou encore les criminels. J’ai eu l’occasion d’utiliser le logiciel Tails ou encore The Amnesic Incognito Live System qui est une distribution GNU/LINUX qui a pour but de protéger son utilisateur pour préserver la vie privée et son anonymat. Celui-ci a la particularité d’être installé sur généralement une clé USB qui peut donc être utilisé de n’importe quel ordinateur partout dans le monde. Toutes les connexions sur ce

réseau sont faites directement sur le réseau Tor ce qui permet un total anonymat en ligne. De plus, il offre une messagerie chiffrée qui est très utilisé par les journalistes par exemple. Mais la plus grande force de ce système et le détachement du système de stockage d'urgence. En effet, un système d'auto-défense a été mis en place pour protéger l'utilisateur, celui-ci permet de retirer la clé USB et d'automatiquement effacer toutes les informations stockées en mémoire tout en sécurité. Cet OS a été utilisé de nombreuses fois par exemple pour de grosses affaires comme avec The Guardian dans l'affaire Snowden. Personnellement, je l'ai déjà utilisé pour envoyer des mails sécurisés ou encore pour surfer sur des réseaux inaccessibles depuis le clear web comme des forums. Dans la vie de tous les jours, j'utilise peu ce type de système de sécurité sur Internet, néanmoins, j'utilise des moteurs de recherche comme Duckduckgo qui sont plus sécurisé que les services de Google. Ce que je fais aussi, c'est l'utilisation d'un logiciel payant (Adguard) qui me protège sur Internet en supprimant les publicités ou arrêtes les pop-ups, il bloque aussi les menaces les mouchards sur des sites web et il embarque aussi une protection DNS. Ce que je fais aussi, si le service me le permet, je bloque l'utilisation du JavaScript sur les sites web. J'utilise aussi de temps en temps pour communiquer des fichiers importants une messagerie chiffrer pour éviter que des informations trop dangereuses soit divulguer.

Pour me protéger face à des cybermenaces, j'utilise souvent une sandbox (mécanisme de sécurité informatique se basant sur l'isolation de composants logiciels, de logiciels ou de groupes de logiciels par rapport à leur logiciel ou système d'exploitation hôte.) généralement lorsque j'ai un doute sur un logiciel que je télécharge en ligne ou des fichiers qui paraissent frauduleux. Le risque qui existe sur cette menace et mon identité en ligne, est que toutes mes informations, stockées en mémoire sur mon ordinateur, soient publiées en ligne. De nos jours, il existe des services en ligne payant qui permet pour environ 300 $ de supprimer toute nos informations présentes sur Internet.

Pour limiter les cyberattaques et les risques que j'encours, je peux directement cacher la caméra de mon ordinateur et le micro directement depuis le hardware de mon ordinateur. J'ai aussi installé un logiciel qui chiffre mes frappes au clavier, ce qui limite par exemple un attaquant de voir mes messages privés ou mes informations personnelles. Généralement, pour déverrouiller un compte, j'utilise l'identification biométrique grâce a la reconnaissance faciale avec Windows hello ou face id avec Apple.

Généralement, j'utilise un environnement centralisé. Pour ma part, j'utilise le système de cloud Apple où je stocke mes photos privées ou encore mes identifiants et mots de passe. Cela limite l'accès à mes informations hors du disque dur de mon ordinateur et permet donc de chiffrer les informations. Pour le professionnel, j'utilise OneDrive qui est très utile dans ma situation qui est généralement sous Windows et est vraiment très ergonomique et très sécurisé.

Néanmoins, comme on nous l'a montré dans différentes fuites sur les services secrets, il est totalement impossible de cacher son identité en ligne avec les grandes entreprises qui ont énormément d'information sur nous et qui peuvent les utiliser peu importe s'il s'agit d'un criminel ou non.

Pour conclure, l'identité numérique et l'e-réputation sont très importantes et peut-être protéger par différents moyens, a commencé par réduire son activité publique sur le web jusqu'à se rendre totalement invisible sur la toile grâce à des logiciels qui nous protègent et nous cache totalement. Malgré tout cela, je pense qu'il est important de nos jours d'avoir une bonne identité numérique afin de s'identifier dans la société tout en limitant au maximum la publication de nos données privées qui je le pense n'ont rien à faire a la vue de tout le monde et pourrait entacher ce qu'on est sur Internet, mais aussi dans la vie réelle.