To Err is Human, To Really Foul up Takes a Computer / L'erreur est humaine, la faute est informatique

You can never be too paranoid with information security / On n'est jamais trop paranoïaque en matière de sécurité informatique

BRYN WILLIAMS-JONES

JUL 11, 2023

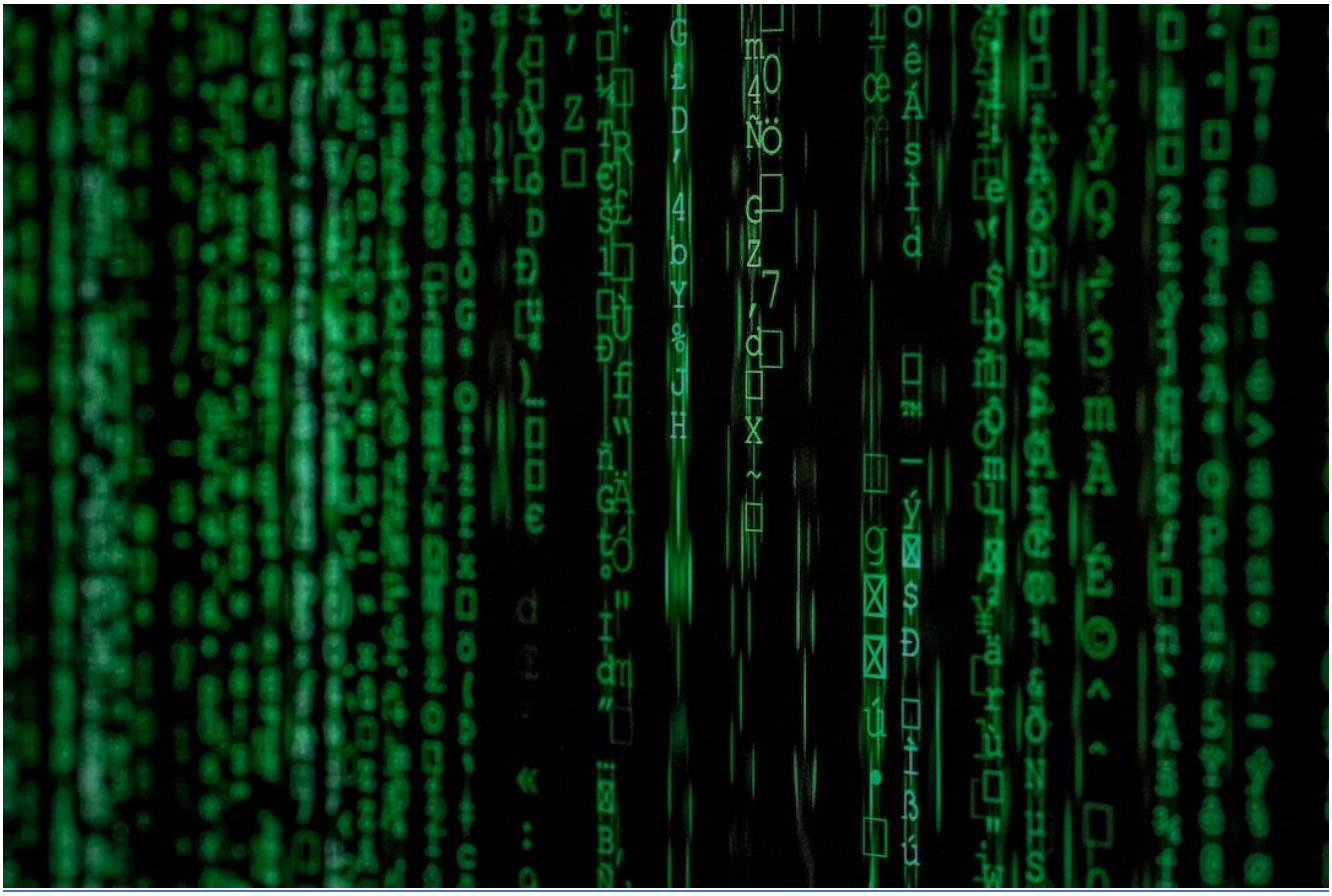

Photo by Markus Spiske on Unsplash

La version française de ce texte figure ci-dessous

Disclaimer: I am a university professor and bioethicist, not a computer security expert. But I'm a techie and interested in information systems and have been using computers since the early 1980s. In my family, I'm the one responsible for computer updates and security. So, my analysis here is based on personal experience, and my recommendations are those of an informed user, not an expert.

Academics, like anyone else, need to have healthy information security habits… but this is often not the case.

Given that many of us spend of our days in front of computers using various computer-based systems (email, research databases, institutional administrative platforms), and sometimes accessing confidential information, the importance of good security should be evident. But as the number and diversity of systems expand, so too do the risks for mistakes, and for data loss and security breaches with far reaching consequences… and many (even most) of these will likely be due to human error.

To err is human

Like anyone else, academics can be lazy and take risky shortcuts with information systems. The most blatant, of course, is the all-too-common use of the same password, or the storing of data on only one computer, or worse yet, on a USB key. A password breach or corrupted file can have a ripple effect across all our personal and professional accounts, and then on to those people with whom we interact. One failure and all can be lost, and with dramatic consequences.

These risks are somewhat mitigated by institutional requirements forcing regular password changes, and automatic data back-ups to cloud storage. But such measures will still be insufficient if our at-work practices are not replicated also with our personal accounts, and if our home information infrastructure does not have similar protections as those offered by our employer, when at the office.

Bad practices are understandable – we are human, after all. Beyond a certain level of complexity, our brains become saturated. Many of us are overwhelmed by the diversity of technologies and systems that we have to use, and thus cannot not fully master. More generally, we can be un(under)informed about security measures and so unable to manage all the different requirements for ensuring information security.

There are so many passwords required for all the different websites and software that we use daily that it's impossible to manage them without using shortcuts, such as using the same password – a better approach would be to use password managers (in our browsers, or separate software). Similarly for data storage, our files may be stored on multiple platforms with different processes and security requirements, and on cloud services, some of which will be outside our home country. Keeping track of all this data, remembering where it is, and ensuring that it's up to date (and protected appropriately) may be extremely difficult.

Thus it's not, in fact, surprising that many students and colleagues still use problematic information practices. While many security risks are due to human limitations or errors, these risks cannot be managed effectively by asking individuals to remember to do something, or to implement additional complex practices.

To mitigate the security risks that result from human behaviour, we need to implement systems that remove the responsibility from individuals. Our security infrastructure – institutional and personal – needs to become invisible, running in the background to protect us, and something for which we need only be minimally involved.

In the not-too-distant future, we should (hopefully) no longer need to worry about passwords and 2-factor-authentication or even individual antivirus protection, because these will have been replaced by much more secure, system-based security measures (software talking to software) that removes individual users from the equation. In the meantime, however, we can each – individually and collectively (through our institutions) – demand and implement best practices (i.e., processes) that mitigate the risk for human error and so maximize the resilience of our information environment.

Securing your system

I have had software and computers infected by viruses, have clicked on links that took me to fraudulent websites, and known people who had been subjected to ransomware attacks and lost their personal and research data. These and other experiences have led me to be relatively paranoid about securing all my and my family's information systems, both at home and at the office.

Updates

One of the simplest but often ignored protections is to ensure that your computer, phone, tablet, etc. are always up to date. Aside from additional features, many of these updates will be security related.

- Ensure that your phone is set to do weekly or automatic app updates; I check and force updates every few days.
- Set your computer/tablet operating system, and all software, to automatically update.
- When you get an update notification, don't delay – do it right away.

Antivirus

Initially designed to protect software, good antivirus systems also offer comprehensive protection for our various online activities.

- Install an up-to-date antivirus system (I use Bitdefender) on all your information platforms – computer, tablet, phone.
- Many of these systems feature additional options, including VPN, protection from ransomware attacks, etc.
- Set the antivirus to systematically verify all emails, downloads, and websites, and to do regular scans.

Privacy

Basic privacy protection should be done at the level of individual platforms. Password protect your computer, phone, table. Set your computer hard drive to be encrypted and set additional encryption on any particularly sensitive folders. Turn on your computer firewall.

For additional privacy protection, install a virtual private network (VPN; I use PIA) to route all internet traffic through a different (and changing) IP address; this makes it extremely difficult to backtrack and identify an individual user.

- Install on your computer, tablet and phone, and use systematically whenever connecting to public Wi-Fi (e.g., library, airport, park) as these are notoriously insecure.
- Use at home to protect your privacy by preventing your service provider from tracking your online activities.
- Consider installing a VPN in the Wi-Fi router to protect your entire home (instead of a client on each computer, phone, etc.). As we move to smart homes that are Internet-connected (e.g., alarm system, thermostat), we increase our online exposure and thus need for protection.

Emails

Beware of phishing scams and ransomware attacks (and other spam) that can be used to gain access to your personal information (e.g., passwords) and files.

- Never click on links in emails nor open attachments if the email looks even remotely suspicious.
- Systematically flag spam and report scams, through your email client.
- Make sure that your antivirus is scanning your email.
- Don't send confidential information as attachments unless you're using encrypted email or a website.

Passwords

One of the more common forms of security breach, that is the risk caused by passwords, can be mitigated by using Password managers, either based in the web browser or as standalone software (I use LastPass).

- Use one complex password (phrase) that you can remember and then generate complex alphanumeric passwords (20+ characters) for all websites and accounts.
- Set an automatic reminder to change (update) passwords on all websites, at least annually.

Backups

As an academic, one of my greatest fears has been losing a document on which I've spent days or more working, due to a bug. My father told me the story of a fellow PhD student who, in the days before computers, lost the single printed copy of his thesis on a plane and so had to start all over from hand-written notes. Many decades later, I came close to having a similar experience. In the last year of my PhD, I had my thesis backed-up on 2 computers and 3 CD-ROMs – the document became corrupted and spread to 4 out of 5 copies. Thankfully, the one uncorrupted copy was only a few days old. Such experiences can and still occur if we're not careful.

Secondary storage

- Backup your computer in real-time by having your desktop and all working files synchronized with cloud storage (e.g., Dropbox, Google Drive, Microsoft OneDrive).
- Set MS Office (Word, PowerPoint, etc.) or equivalent to save every 5 minutes.
- Add an external hard drive that does daily backups of your entire computer, both at home and at the office.

Uninterrupted Power Supply (UPS) Batteries

Power failures are very problematic, both due to the loss of work and the damage they can cause to electronics. In my neighbourhood, power outages are sufficiently frequent that we've installed multiple backup batteries at home. Plugging the computer and modem/router into a UPS battery will ensure that a power surge or failure does not fry your electronics and gives you between a few minutes to even a few hours to finish what you're doing. My setup is the following:

- Desktop computer UPS (lasts 3+ hrs): APC UPS Back-UPS Pro (BX1500M)
- Modem/router UPS (because not near our computers) so internet doesn't drop: 600VA APC Back-UPS (BE600M1)

I've lost power in the middle of a Zoom meeting and only noticed because the lights went out!
After a major power outage in Montreal in April 2023, I ordered an additional portable battery (which can also work as a UPS) to charge cellphones, tablets, laptops (BLUETTI Portable Power Station EB3A) so that we have connectivity for 5-8 hours.

Conclusions

You can never be too paranoid when it comes to security and protecting your information systems. Now an integral part of our daily lives, these systems unfortunately still require an undue amount of individual responsibility to ensure their security, and that is a major source of risk. Nonetheless, knowing that these requirements can become unmanageable if treated individually, we can implement good practices – i.e., systems or processes that do not require much attention – that make them more secure. In so doing, we use information systems to mitigate rather than augment the risk of human error.

Avertissement : je suis professeur d'université et bioéthicien, et non expert en sécurité informatique. Mais je suis un technophile, je m'intéresse aux systèmes d'information et j'utilise des ordinateurs depuis le début des années 1980. Dans ma famille, c'est moi qui suis responsable des mises à jour et de la sécurité des ordinateurs. Mon analyse est donc basée sur mon expérience personnelle et mes recommandations sont celles d'un utilisateur averti, pas d'un expert.

Les universitaires, comme tout le monde, doivent avoir de bonnes habitudes en matière de sécurité de l'information... mais ce n'est souvent pas le cas.

Étant donné que beaucoup d'entre nous passent leurs journées devant des ordinateurs à utiliser divers systèmes informatiques (courriels, bases de données de recherche, plateformes administratives institutionnelles) et qu'ils accèdent parfois à des informations confidentielles, l'importance d'une bonne sécurité devrait être évidente. Mais plus le nombre et la diversité des systèmes augmentent, plus les risques d'erreurs, de pertes de données et de failles de sécurité sont importants... et beaucoup (voire la plupart) d'entre eux seront probablement dus à l'erreur humaine.

L'erreur est humaine

Comme tout le monde, les universitaires peuvent être paresseux et prendre des raccourcis risqués avec les systèmes d'information. Le plus flagrant, bien sûr, est l'utilisation trop fréquente du même mot de passe, ou le stockage de données sur un seul ordinateur, ou pire encore, sur une clé USB. Une faille dans le mot de passe ou un fichier corrompu peut avoir un effet d'entraînement sur tous nos comptes personnels et professionnels, puis sur les personnes avec lesquelles nous interagissons. Une seule défaillance et tout peut être perdu, avec des conséquences dramatiques.

Ces risques sont quelque peu atténués par les exigences institutionnelles imposant des changements réguliers de mot de passe et des sauvegardes automatiques de données sur un système de stockage en nuage. Mais ces mesures resteront insuffisantes si nos pratiques au travail ne sont pas reproduites sur nos comptes personnels et si notre infrastructure d'information domestique ne dispose pas de protections similaires à celles offertes par notre employeur lorsque nous sommes au bureau.

Les mauvaises pratiques sont compréhensibles – nous sommes humains, après tout. Au-delà d'un certain niveau de complexité, notre cerveau est saturé. Beaucoup d'entre nous sont dépassés par la diversité des technologies et des systèmes que nous devons utiliser et que nous ne pouvons donc pas maîtriser complètement. Plus généralement, nous pouvons être mal informés sur les mesures de sécurité et donc incapables de gérer toutes les différentes exigences pour assurer la sécurité de l'information.

Les mots de passe requis pour les différents sites web et logiciels que nous utilisons quotidiennement sont si nombreux qu'il est impossible de les gérer sans recourir à des raccourcis, comme l'utilisation du même mot de passe – une meilleure approche consisterait à utiliser des gestionnaires de mots de passe (dans nos navigateurs, ou dans des logiciels distincts). De même, en ce qui concerne le stockage des données, nos fichiers peuvent être stockés sur plusieurs plateformes avec des processus et des exigences de sécurité différente, ainsi que sur des services en nuage, dont certains se trouvent en dehors de notre pays d'origine. Il peut être extrêmement difficile de garder la trace de toutes ces données, de se rappeler où elles se trouvent et de s'assurer qu'elles sont à jour (et protégées de manière appropriée).

Il n'est donc pas surprenant que de nombreux étudiants et collègues utilisent encore des pratiques problématiques en matière d'information. Si de nombreux risques de sécurité sont dus à des limitations ou à des erreurs humaines, ces risques ne peuvent pas être gérés efficacement en demandant aux individus de se souvenir de faire quelque chose ou de mettre en œuvre des pratiques complexes supplémentaires.

Pour atténuer les risques de sécurité résultant du comportement humain, nous devons mettre en place des systèmes qui déchargent les individus de leur responsabilité. Notre infrastructure de sécurité – institutionnelle et personnelle – doit devenir invisible, fonctionner en arrière-plan pour nous protéger et ne nécessiter qu'une implication minimale de notre part.

Dans un avenir pas si lointain, nous devrions (espérons-le) ne plus avoir à nous soucier des mots de passe et de l'authentification à deux facteurs, ni même de la protection antivirus individuelle, car ils auront été remplacés par des mesures de sécurité beaucoup plus sûres, basées sur le système (logiciel communiquant avec le logiciel), qui éliminent les utilisateurs individuels de l'équation. En attendant, nous pouvons tous – individuellement et collectivement (par l'intermédiaire de nos institutions) – exiger et mettre en œuvre les meilleures pratiques (c'est-à-dire les processus) qui réduisent le risque d'erreur humaine et maximisent ainsi la résilience de notre environnement d'information.

Sécuriser son système

J'ai eu des logiciels et des ordinateurs infectés par des virus, j'ai cliqué sur des liens qui me conduisaient vers des sites web frauduleux, et j'ai connu des personnes qui avaient été victimes d'attaques de rançongiciel et avaient perdu leurs données personnelles et leurs données de recherche. Ces expériences et d'autres m'ont amené à être relativement paranoïaque en ce qui concerne la sécurisation de tous mes systèmes d'information et de ceux de ma famille, à la fois à la maison et au bureau.

Mises à jour

L'une des protections les plus simples, mais souvent ignorées, consiste à s'assurer que son ordinateur, son téléphone, sa tablette, etc. sont toujours à jour. Outre les fonctionnalités supplémentaires, bon nombre de ces mises à jour sont liées à la sécurité.

- Assurez-vous que votre téléphone est configuré pour effectuer des mises à jour hebdomadaires ou automatiques des applications ; je vérifie et force les mises à jour tous les deux jours.
- Réglez le système d'exploitation de votre ordinateur ou de votre tablette, ainsi que tous les logiciels, de manière à ce qu'ils soient mis à jour automatiquement.
- Lorsque vous recevez une notification de mise à jour, ne tardez pas, faites-la immédiatement.

Antivirus

Initialement conçus pour protéger les logiciels, les bons systèmes antivirus offrent également une protection complète pour nos diverses activités en ligne.

- Installez un système antivirus à jour (j'utilise Bitdefender) sur toutes vos plateformes d'information – ordinateur, tablette, téléphone.
- Beaucoup de ces systèmes proposent des options supplémentaires : VPN, protection contre les attaques de rançongiciel, etc.
- Paramétrez l'antivirus pour qu'il vérifie systématiquement tous les courriels, les téléchargements et les sites web, et pour qu'il effectue des analyses régulières.

Protection de la vie privée

La protection de base de la vie privée doit se faire au niveau des plateformes individuelles. Protéger son ordinateur, son téléphone, sa tablette par un mot de passe. Paramétrer le disque dur de l'ordinateur pour qu'il soit crypté et paramétrer un cryptage supplémentaire pour les dossiers particulièrement sensibles. Activer le pare-feu de votre ordinateur.
Pour une protection supplémentaire de la vie privée, installer un réseau privé virtuel (VPN ; j'utilise PIA) pour acheminer tout le trafic internet via une adresse IP différente (et changeante) ; cela rend extrêmement difficile le retour en arrière et l'identification d'un utilisateur individuel.

- Il faut l'installer sur son ordinateur, sa tablette et son téléphone, et l'utiliser systématiquement lorsqu'on se connecte à un réseau Wi-Fi public (bibliothèque, aéroport, parc, etc.), car il est notoire que ces réseaux ne sont pas sécurisés.
- Utiliser le VPN à la maison pour protéger sa vie privée en empêchant son fournisseur d'accès de suivre ses activités en ligne.
- Envisager d'installer un VPN dans le routeur Wi-Fi pour protéger l'ensemble de la maison (au lieu d'un client sur chaque ordinateur, téléphone, etc.). Les maisons intelligentes connectées à Internet (système d'alarme, thermostat, etc.) augmentent notre exposition en ligne et donc notre besoin de protection.

Courriels

Attention aux escroqueries par hameçonnage et aux attaques de rançongiciel (et autres pourriels) qui peuvent être utilisées pour accéder à des informations personnelles (ex. : des mots de passe) et à des fichiers.

- Ne jamais cliquer sur les liens contenus dans les courriels ni ouvrir les pièces jointes si le courriel semble le moindrement suspect.
- Signaler systématiquement les pourriels et les escroqueries par l'intermédiaire de son client de messagerie.
- S'assurer que l'antivirus analyse le courrier électronique.
- N'envoyez pas d'informations confidentielles sous forme de pièces jointes, sauf si vous utilisez un courriel ou un site web crypté.

Mots de passe

L'une des formes les plus courantes d'atteinte à la sécurité, à savoir le risque causé par les mots de passe, peut être atténuée par l'utilisation de gestionnaires de mots de passe qu'ils soient intégrés au navigateur web ou qu'ils constituent un logiciel autonome (j'utilise LastPass).

- Utiliser un mot de passe complexe (phrase) dont on peut se souvenir, puis générer des mots de passe alphanumériques complexes (20 caractères ou plus) pour tous les sites web et comptes.

- Définir un rappel automatique pour changer (mettre à jour) les mots de passe sur tous les sites web, au moins une fois par an.

Sauvegardes

En tant qu'universitaire, l'une de mes plus grandes craintes est de perdre un document sur lequel j'ai passé des jours ou plus à travailler, à cause d'un bogue. Mon père m'a raconté l'histoire d'un doctorant qui, à l'époque où les ordinateurs n'existaient pas encore, avait perdu l'unique exemplaire imprimé de sa thèse dans un avion et avait dû tout recommencer à partir de notes manuscrites. Plusieurs décennies plus tard, j'ai failli vivre une expérience similaire. Au cours de la dernière année de mon doctorat, j'avais sauvegardé ma thèse sur deux ordinateurs et trois CD-ROM – le document s'est corrompu et s'est propagé à quatre des cinq copies. Heureusement, la seule copie non corrompue n'avait que quelques jours. De telles expériences peuvent se produire et se produisent encore si nous ne sommes pas prudents.

Stockage secondaire

- Sauvegardez votre ordinateur en temps réel en synchronisant votre bureau et tous vos fichiers de travail avec un système de stockage en nuage (ex. : Dropbox, Google Drive, Microsoft OneDrive).
- Configurez MS Office (Word, PowerPoint, etc.) ou équivalent pour qu'il sauvegarde toutes les 5 minutes.
- Ajoutez un disque dur externe qui effectue des sauvegardes quotidiennes de l'ensemble de l'ordinateur, à la fois à la maison et au bureau.

Batteries d'alimentation sans interruption (ASI)

Les pannes de courant sont très problématiques, à la fois en raison de la perte de travail et des dommages qu'elles peuvent causer aux appareils électroniques. Dans mon quartier, les coupures de courant sont suffisamment fréquentes pour que nous ayons installé plusieurs batteries de secours à la maison. En branchant l'ordinateur et le modem/routeur sur une batterie ASI, on s'assure qu'une surtension ou une panne de courant ne grille pas les appareils électroniques et on dispose de quelques minutes, voire de quelques heures, pour terminer ce que l'on est en train de faire. Ma configuration est la suivante :

- ASI pour ordinateur de bureau (dure plus de 3 heures) : APC UPS Back-UPS Pro (BX1500M)
- ASI pour modem/routeur (parce qu'il n'est pas près de nos ordinateurs) pour que l'internet ne tombe pas en panne : 600VA APC Back-UPS (BE600M1).

Il m'est arrivé de subir une panne de courant au milieu d'une réunion Zoom et de ne m'en apercevoir que parce que les lumières s'étaient éteintes!

Après une grande panne d'électricité à Montréal en avril 2023, j'ai commandé une batterie portable supplémentaire (qui peut également fonctionner comme ASI) pour charger les téléphones portables, les tablettes et les ordinateurs portables (BLUETTI Portable Power Station EB3A) afin que nous ayons une connectivité pendant 5 à 8 heures.

Conclusions

On n'est jamais trop paranoïaque en matière de sécurité et de protection des systèmes informatique. Devenus partie intégrante de notre vie quotidienne, ces systèmes nécessitent malheureusement encore une part excessive de responsabilité individuelle pour assurer leur sécurité, ce qui constitue une source de risque important. Néanmoins, sachant que ces exigences peuvent devenir ingérables si elles sont traitées individuellement, nous pouvons mettre en œuvre de bonnes pratiques – c'est-à-dire des systèmes ou des processus qui ne nécessitent pas beaucoup d'attention – qui les rendent plus sûrs. Ce faisant, nous utilisons les systèmes informatiques pour atténuer le risque d'erreur humaine plutôt que de l'augmenter.