7-2018

Safe and secure? Not without digital hygiene

Kunaciilan Nallappan

Safe and Secure? Not Without Digital Hygiene

By Kunaciilan Nallappan

A generation ago, one would scoff at the thought of renting clothes or carpooling with strangers. These days, however, it seems like the sharing economy has taken the world by storm. From ride-sharing to lodging, consumers are now looking at alternatives to traditional services and businesses.

In Singapore, the enthusiasm for new technologies is holding steady. It was reported that Singaporeans spend more than half of their day,[1] or an average of 12 hours and 42 minutes, on digital devices. Of that time, about 3 hours and 12 minutes are spent staring into the screens of their mobile phones.

However, as with every economic disruptor, this often means a gap with reality. Mobile payments and cloud storage may come with convenience and benefits, but they can also open the doors to digital pitfalls such as cyber risk.

COST VS. BENEFIT

When it comes to cybersecurity, one could presently argue that this is a chicken-and-egg situation—should we not upload our data onto cyberspace, there would be nothing to secure, and therefore nothing to worry about.

Singaporeans spend more than half of their day, or an average of 12 hours and 42 minutes, on digital devices. Of that time, about 3 hours and 12 minutes are spent staring into the screens of their mobile phones.

However, this is not really possible, as our growing reliance on the speed and convenience of apps comes at a price. People are generally willing to offer personal information just to shave off precious *seconds* of waiting. This is great, until they realise that the sharing economy is also a treasure trove for cybercriminals who can tap into an entire ecosystem of authenticated devices and data that are interconnected.

Let us not forget the lessons of 2017, the year in which businesses bore grave consequences for mismanaging their cybersecurity strategies. That year, unpatched Windows systems caused disruptions to many Asian governments and businesses, as WannaCry rapidly spread to over 150 countries, and infected more than 200,000 systems.[2] The institutions' resulting losses were staggering, too: US$4 billion[3] from the shutting down of operations.

Back in Singapore, bike-sharing service provider oBike also suffered a global security breach[4] in which its users' data—names, email addresses, profile pictures, biking routes and mobile numbers—were leaked online.

However, though cybersecurity is a widely discussed topic in the news and social media, the conversation is still largely focused on society's vulnerability to attacks and the responses of governments and relevant institutions. Rarely included in the discussion is the question of how well-versed *individuals* themselves are at managing cybersecurity.

That needs to change.

CYBERSECURITY AS A WAY OF LIFE?

Recognising cybersecurity as one of the most pressing issues of our time, governments all around the world have stepped up in their bid to thwart its threats. For example, the World Economic Forum (WEF) announced a new Global Centre for Cybersecurity. Headquartered in Geneva and operational since March 2018, the Centre is the "first global platform"[5] for governments, businesses, experts and law enforcement agencies to collaborate on cybersecurity challenges.

WannaCry rapidly spread to over

150

countries and infected more than

200,000

systems

People are generally willing to offer personal information just to shave off precious seconds of waiting. This is great, until they realise that the sharing economy is also a treasure trove for cybercriminals who can tap into an entire ecosystem of authenticated devices and data that are interconnected.

Nonetheless, depending solely on government policies and initiatives is not enough. To create a cyber-safe environment and foolproof future generations, individuals—especially heavy users of tech—have to do their part to ensure that cybersecurity management becomes a way of life.

Tech is a big part of our lives, especially for millennials, who grew up in the age of the Internet, smartphones and social media. But while the youth may be plugged in to the latest apps and devices, how vigilant are they about cyber safety? Additionally, are adults necessarily more educated about "digital hygiene"?

No matter our level of tech usage, how should we manage our personal cyber risk?

CYBERSECURITY VOCABULARY:

COMMON TERMS YOU NEED TO KNOW

TERM	DEFINITION
Access control	Selective restriction of access to a place or other resource, including the information it stores
Authenticity	Assurance that a message, transaction or other exchange of information is from the source it claims to be
Authorisation	A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource
Behaviour monitoring	Observing activities of users, information systems and processes, and measuring the activities against organisational policies and rules, baselines of normal activity, thresholds and trends
Compliance training	The process of educating employees on laws, regulations and company policies that apply to their day-to-day job responsibilities
Data-mining	The process or techniques used to analyse large sets of existing information to discover previously unrevealed patterns or correlations
Distributed denial of service (DDoS)	An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources
Digital footprint	A trail of data you create while using the Internet. It includes the websites you visit, emails you send and information you submit to online services
Identity and access management	The methods and processes that enable the right individuals to access the right resources at the right times and for the right reasons
Machine learning and evolution	A field concerned with designing and developing artificial intelligence algorithms for automated knowledge discovery and innovation by information systems
Malicious code	Programme code intended to perform an unauthorised function or process that will have an adverse impact on the confidentiality, integrity or availability of an information system
Multi-factor authentication (MFA)	A security mechanism in which individuals are authenticated through more than one required security and validation procedure. MFA is built from a combination of physical, logical and biometric validation techniques used to secure a facility, product or service.
Password fatigue	The feeling induced by trying to remember too many passwords
Phishing	A digital form of social engineering to deceive individuals into providing sensitive information
Spyware	Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner
Security automation	The use of information technology in place of manual processes for cyber incident response and management

6 STEPS TO BETTER DIGITAL HYGIENE

#1 Audit Digital Subscriptions

According to Nielsen's *Millennials on Millennials* report,[6] young people move on quickly from one digital service to the next. However, they also tend to have multiple subscription-based applications set on an auto-renewal basis, not so much due to customer loyalty, but to avoid having to manually renew their Netflix or Spotify subscriptions every month.

It is common for most digital services to request credit card credentials to access trial periods, which are then billed straight into a user's regular subscriptions. So if you are not prudently and regularly checking your bank statements or your Google Play Store and App Store billings, you may end up paying a dear price for the perceived convenience of an automatically renewing subscription—whether you continued to use a service or not.

#2 Provide Tools to Create Strong, Secure Passwords

Time and again, we read reminders on strengthening our passwords, and yet this advice often goes unheeded. SplashData, a company that creates applications for password management and security, conducted research on the worst passwords of

2017,[7] based off more than five million leaked passwords. Their findings were astounding—close to three per cent of people used the worst password on the list (123456), with almost 10 per cent having used one of the worst 25.

It was unsurprising, then, that the cause behind the Equifax breach[8] in Argentina—which exposed sensitive personal information of thousands of customers' national identity numbers—was an online employee tool that had "admin" as both the login and password.

While the average person may choose to ignore the perils of weak passwords, businesses must seriously consider implementing multi-factor authentication (MFA) via application services that provide an easy integration with numerous MFA vendors. At F5,[9] where I am based, we offer application access solutions[10] that provide businesses and their users with greater authentication processes—they have the choice of second- and even third-factor authentication.

#3 Manage Your Secured Passwords

Now that we have established strong and unique passwords for each service, boosted by an added security layer through MFA, what's next? Given how user password fatigue is a big contributor to malicious phishing attacks, how can we store our passwords safely?

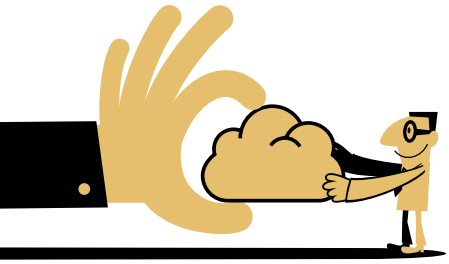
Given how user password fatigue is a big contributor to malicious phishing attacks, how can we store our passwords safely? The answer is a password manager.

The answer is a password manager. Living in your browser and acting as a digital gatekeeper, a password manager fills in your login info when you need to get on a certain site, and eliminates the need to track dozens of passwords. With an array of services that allows you to store your passwords locally or in the cloud, users are only required to remember one master password for the manager itself, with everything else managed internally. Some of the more popular password managers available in the market include 1Password,[11] LastPass,[12] and Dashlane.[13]

#4 Embrace The Cloud Services

The good news is, the proliferation of cloud-based services is not slowing down anytime soon. In F5's recent *State of Application Delivery* report,[14] it was found that 84 per cent of Asia Pacific respondents use multiple clouds. This means that many people subscribe to several external cloud providers and use a mix of cloud and dedicated (on-premise) IT resources.

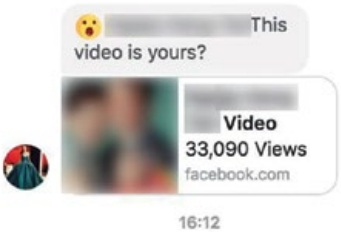
Whether in the classroom or at the workplace, digital presentations are now favoured due to the ease of sharing among one's peers. It is now common for lecturers and subordinates to share their notes and presentations via Google Drive or Dropbox, while online presentation tools such as Prezi[15] or Google Slides[16] offer contributors many more options in terms of tracking changes in real time.



The switch from USB drives to cloud-sharing services also lessens the risks of accidentally introducing a virus to an organisation's network. My own team at F5 has transitioned away from USB drives to cloud-based sharing solutions such as SharePoint, Dropbox and OneDrive. This has helped us eliminate the risk of USB drives falling into the wrong hands, being lost accidentally or worse still, inadvertently spreading malware.

Going forward, with corporations progressing in their digital transformation (automation, orchestration, digital enablement for productivity purposes), they will very likely start consuming public (IaaS) cloud with greater ferocity than in the past.

#5 Beware Of Phishing (It Gets Personal)



Screengrab of the suspicious link sent via Facebook Messenger

According to Ponemon Institute's 2016 *Cost of Data Breach Study*,[17] most data breaches come from within, i.e., are caused by employees with no intention of harming the organisation. Of the cited 874 incidents, 568 were due to employee or contractor negligence; 85 by outsiders using stolen credentials; and 191 by malicious employees and criminals.

Most schools and companies have now placed compulsory compliance training for their staff and members. In F5, for instance, every full-time employee and contractor has to undergo a compulsory annual security training to ensure that they understand the need for digital hygiene as well as the various security risks they may encounter at the workplace, including phishing.

However, in spite of education and training, there will always be a few who make mistakes.

Just recently, Facebook Messenger users in Singapore reported a resurgence in a new round of hoax messages[18] being sent, where victims were taken to a page that looks like a playable movie. When they clicked on the fake playable movie, malware then redirected them to a set of websites which exposed their browser, operating system and other vital information.

According to Ponemon Institute's 2016 Cost of Data Breach Study, most data breaches come from within, i.e., are caused by employees with no intention of harming the organisation ... data security is still compromised every time employees share and spread information about themselves on the Internet. Social media companies expend tremendous effort to encourage people to join and post information about themselves. This makes it easy for phishers to pull information together into comprehensive professional dossiers.

Phishing is a way that attackers use to collect data about an organisation's employees.[19] Since phishers tend to target users in a specific company, they need to know who exactly works there before they strike.

So even though a corporation's IT team may put in great effort to prevent attacks, data security is still compromised every time employees share and spread information about themselves on the Internet. Social media companies expend tremendous effort to encourage people to join and post information about themselves. This makes it easy for phishers to pull information together into comprehensive professional dossiers.

The lesson here? Think before you volunteer information about yourself and your work, and limit the number of websites where you do this.

#6 Watch Your Digital Footprint

A recent Ernst and Young survey[20] found that privacy is a dominant concern among users. In that same study, a vast 81 per cent of respondents worried about how organisations collect, store and use data about them, and 75 per cent wanted the government to exert greater control and ensure more transparency in the process.

Unfortunately, unless you have fully disconnected yourself from all forms of web services, there is a good chance that you have already amassed a huge digital footprint. From search engines to web browsers to your mobile phone, data retention policies have been exasperating consumers for years now.

Therefore, before you click on that "I Agree" button, it would be wise to read the different clauses presented to you by each Internet service you are engaging. Popular search engines store your data through logs, which monitors your sessions on their servers. Cell service providers also keep track of your data, from the numbers you dial to your text messages. Finally, while we are mostly aware that our mobile phones are keeping tabs on us, do we actually know how extensive this data retention is? Whether you have an iOS or an Android device, Apple and Google can collect data about how you use it: the places you go, the apps you run, and the search queries you type into the web browser.

It is all legal, by the way, since you signed your consent by hitting that "I Agree"[21] button. However, you can still limit the extent of data-tracking by fully exploring your options on your mobile devices. Some ways to do this include turning off the location data for certain apps, resetting the advertising identifier to wipe all the data that's been collected on your iPhone, and switching off the Google Location History, which lets you stop location data from being sent back to Google.

Unfortunately, unless you have fully disconnected yourself from all forms of web services, there is a good chance that you have already amassed a huge digital footprint.

FOOLPROOFING CYBERSECURITY FOR FUTURE GENERATIONS

As a parent to two teenage kids who grew up with technology, it amazes as well as worries me to see how technologically dependent our future generations will be. Unlike their parents and grandparents, Generation Z will be the true digital natives since they only recognise a world with touch screens, social media and apps.

space is important as it enables people to enjoy the convenience brought about by technology.

As newer, more sophisticated technologies emerge, so too are increasingly complex threats. Trends and predictions last no more than three months at a go, and both individuals and corporations have to constantly be on guard against imminent attacks. Thankfully there already exist solutions that have enough mobility and agility to advance in tandem with complex threats.

But when it comes to future-proofing the platforms and the data security of tomorrow's generation, it is up to everyone *today* to take the first step.

The onus is upon us to ensure we cultivate a culture of security where everyone knows the tactics of cybersecurity management and how to avoid being compromised. This safe space is important as it enables people to enjoy the convenience brought about by technology.

In fact, 92 per cent of children in the United States[22] have a digital footprint, and it is a matter of time before this transposes over to the Asia Pacific region.

What this also means is that young people will become accustomed or almost "desensitised" to cybersecurity breaches. It is a real but worrying possibility that we might be approaching a new era of oversharing and personal data breaches, and the end of personal privacy.

To avoid such an outcome, the onus is upon us to ensure we cultivate a culture of security where everyone knows the tactics of cybersecurity management and how to avoid being compromised. This safe

Notes

1 Lin Yangchen, "People in Singapore Spend Over 12 Hours on Gadgets Daily: Survey", *The Straits Times*, 3 April 2017, at http://www.straitstimes.com/singapore/12hr-42min-connected-for-hours

2 Andrew Liptak, "The WannaCry Ransomware Attack Has Spread to 150 Countries", *The Verge*, 14 May 2017, at https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

3 Jonathan Berr, "'WannaCry' Ransomware Attack Losses Could Reach $4 Billion", *CBS News*, 16 May 2017, at https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

4 Kevin Kwang, "Bike-sharing Provider oBike Suffers Global Data Breach", *Channel NewsAsia*, 7 December 2017, at https://www.channelnewsasia.com/news/technology/bike-sharing-provider-obike-suffers-global-data-breach-9477588

5 Kevin Kwang, "WEF Launches Global Centre for Cybersecurity, Hopes for International Collaboration", *Channel NewsAsia*, 25 January 2018, at https://www.channelnewsasia.com/news/technology/wef-launches-global-centre-for-cybersecurity-hopes-for-9894458

6 Nielsen, *Millennials on Millennials—Digital Music and Communication*, 21 August 2017, at http://www.nielsen.com/us/en/insights/reports/2017/millennials-on-millennials-digital-music-and-communication.html

7 Allie Porter, "Worst Passwords of 2017", *The Press Democrat*, 26 December 2017, at http://www.pressdemocrat.com/lifestyle/7806309-181/worst-passwords-of-2017?sba=AAS

8 "Equifax Had 'Admin' as Login and Password in Argentina", *BBC*, 13 September 2017, at http://www.bbc.com/news/technology-41257576

9 F5 website, at https://f5.com

10 F5, "Security Solutions: Identity Federation and Remote Access", at https://f5.com/products/security/identity-and-access-management

11 1Password website, at https://1password.com

12 LastPass website, at https://www.lastpass.com

13 Dashland website, at https://www.dashlane.com

14 F5, *The State of Application Delivery* 2018 Report, at https://f5.com/about-us/news/the-state-of-application-delivery

15 Prezi website, at https://prezi.com

16 Google Slides, at https://www.google.com/slides/about

17 Ponemon Institute, *2016 Cost of Data Breach Study: Global Analysis*, at https://app.clickdimensions.com/blob/softchoicecom-anjf0/files/ponemon.pdf

18 Diane Leow, "This Video Is Yours? Facebook Messages Rigged with Malware Resurface in Singapore", *Channel NewsAsia*, 9 January 2018, at https://www.channelnewsasia.com/news/singapore/this-video-is-yours-facebook-messages-rigged-with-malware-9844748

19 Ray Pompon, "Phishing For Information, Part 2: How Attackers Collect Data about Your Employees", F5.com, at https://f5.com/labs/articles/threat-intelligence/identity-threats/phishing-for-information-part-2-how-attackers-collect-data-about-your-employees

20 EY, "Savvy Singapore: Decoding a Digital Nation", at http://www.ey.com/sg/en/services/advisory/ey-savvy-singapore-decoding-a-digital-nation

21 Apple, "Privacy Policy", at https://www.apple.com/sg/legal/privacy/en-ww

22 Erik Qualman, "Social Media Video 2013", YouTube, 7 November 2012, at https://www.youtube.com/watch?v=QUCfFcchw1w

Kunaciilan Nallappan *is F5's Regional Vice President of Marketing (Asia Pacific, China and Japan). Based in Singapore, he is responsible for driving marketing strategies and programmes to increase F5's brand awareness and market penetration in the Asia Pacific region. Kuna holds an Engineering Degree from the National University of Singapore and an MBA from the Nanyang Business School, Singapore. He can be reached at* ***K.Nallappan@F5.com***