### **Mitigating Personal Information exposure on the web**

Due to the vast and instantaneous improvements of technology in today's times (Ramey, 2012), there is also an increasing problem with protecting our information (Chao, Pham & Seregine, n.d.). We aim to evaluate and address how to hinder the unwanted attention and knowledge of our personal information; particularly interested in how companies such as social media outlets and banks handle our information, how we use our data accompanied by the way we handle our online footprint and also the ways in which people can be ‘caught' out by scammers and such.

The worldwide web; first appearance on the internet in 1993 to present day 2018, has gone through numerous changes. Through the invention of social media, most notably Facebook in 2012 (Presse, 2014); and online banking wherein 2006 about 80% of American banks offered online services (Sarreal, 2018); also the development of phishing and scams such as the "419" scam (Campbell, 2008). We will look at the various approaches that have been taken to reduce the risks of letting personal information loose on the world wide web.

#### **Companies: Social Media and Banking Services**

With the world wide web being more prominent than ever in our daily lives, companies have a big presence on the scene (Williams-Grut, 2017). Due to the expanding number of companies switching and adding online services, it comes with problems. The main area of focus that we will look into our online stores, on account of personal banking information and their handling of storage and security. In 2014, Home Depot had a breach on more than ‘56,000,000' credit card details (Roberts, 2017); this particular event parked my interest in looking at how companies deal with data breaches and any possible advice they give to their users.

Recently a Facebook breach had happened in mid-Sept 2018 (Isaac & Frenkel, 2018); Facebook is notorious for rewarding anyone, "without malicious intent"; to hack into their system. In one example, they paid $10,000 USD to a person who hacked into their Instagram services (Forsell, 2016). After looking at one particular source ("Data Protection and how to prevent Data Breaches", 2018), it suggests that there is a need for up-to-date security software, regular risk assessments, encryptions and data backups, staff training and awareness on the matter as well as making sure vendors and partners maintain higher or the same equivalent safety breach protocols as they should.

We're also looking into how banks and any other financial business deal with data breach as well. A notable infamous data breach was in June 2005; possibly the "largest data security breach to date" (Evers, 2005), due to a security breach of a third-party processor of card payment transactions, nearly 40 million card accounts were exposed to potential fraud due to the lack of protocols from CardSystems Solutions (Sahadi, 2005). Due to various discoveries of holding data in unencrypted forms and that their network was accessible to hackers (Dash, 2005), various credit card companies have dropped the company. This was one of the few financial hacks that would be surpassed by many incidents like these.

#### **Personal Security: Measures taken by Yourself**

Various personal information can actually be lost due to a user not taking their own security measures by putting stronger passwords (Sandler, 2018); due to this, California has proposed a law that makes having "weak" passwords illegal in 2020 ("Weak passwords illegal in California from 2020", 2018). Various ideas support making your passwords complicated; like constructing them from a sentence or a "nonsense word". They also support the idea of not using numbers relevant to you, such as your birthday or your address. Also recommended that you should never let your browser remember your passwords either. (Buist, 2014).

As mentioned earlier when looking upon online banking services, we also look at phishing. Phishing is a way of collecting personal information (most particularly banking details) through the means of websites and emails (Fruhlinger, 2018). Notable cases include Hillary Clinton's campaign chair John Podesta gave away his Gmail password in 2016 (Krawchenko, 2016), and when employees at University of Kansas gave away access to their paycheck deposit information, ultimately they lost their pay (Lowry, 2016). There are two main types of Phishing techniques; giving out personal information, and downloading suspicious malware. A good indication that you're being ‘phished', through handing over information, is when the website looks like a ‘knock-off' of the original company and such, same can be said about emails. Prevention of being scammed by phishing emails can come from just checking the email address and any website links for spelling errors, not posting any personal information on social media, checking if you actually use or have accounts with the service company or brand, and even just calling up the actual company from known phone numbers (Fruhlinger, 2018). Various methods can also call for checking on the security of the website by putting in fake passwords, "A legitimate site will not accept the fake, but the phishing site will". And also calling for the aided use of updated antivirus and firewall software to minimize the risk of being scammed ("10 Tips for Phishing Prevention", 2006).

#### **Conclusion**

Having looked at various methods of how the modern world is being scammed online, there are numerous ways to hinder the chances of this happening. Through the means of trusting better companies and partners with your personal data, to making sure you practice not leaving a very open online footprint on the world wide web. At the end of the research, it's proven that the most effective way to not be scammed is to practice habits yourself, for instance checking on the validity of the website or email (checking for spelling errors and putting in fake passwords), having updated software to tackle viruses and malicious websites.

As the world is evolving and the way we use technology is always increasing and renovating, the same approach can be said the same for scams; thus meaning that we will have to keep looking for more ways to not be caught out and not be scammed.

##### 

##### **Bibliography**

Ramey, K. (2012). Technological Advancements and Their Effects on Humanity - Use of Technology. Retrieved from https://www.useoftechnology.com/technological-advancements-effects-humanity/

Chao, T., Pham, T., & Seregine, M. The Dangers of Technological Development. Retrieved from https://cs.stanford.edu/people/eroberts/cs181/projects/technology-dangers/issues.html

Internet 101 What is the Internet?. (2017). Retrieved from http://www.just.edu.jo/~mqais/cis99/PDF/Internet.pdf

Presse, A. (2014). A 25-Year Timeline Of The World Wide Web. Retrieved from https://www.businessinsider.com/a-25-year-timeline-of-the-world-wide-web-2014-3?IR=T

Sarreal, R. (2018). History of Online Banking: How Internet Banking Went Mainstream. Retrieved from https://www.gobankingrates.com/banking/banks/history-online-banking/

Campbell, N. (2008). BBC - Watchdog: The 419 scam. Retrieved from http://www.bbc.co.uk/blogs/watchdog/2008/10/the\_419.html

Williams-Grut, O. (2017). 'What we're seeing is a revolution': How the internet is remaking the British High Street. Retrieved from http://uk.businessinsider.com/future-british-high-street-internet-brexit-retail-2017-8

Roberts, J. (2017). http://fortune.com. Retrieved from http://fortune.com/2017/03/09/home-depot-data-breach-banks/

Isaac, M., & Frenkel, S. (2018). Facebook Security Breach Exposes Accounts of 50 Million Users. Retrieved from https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

Forsell, T. (2016). Facebook pays $10,000 to 10-year-old Instagram Hacker. Retrieved from https://www.reuters.com/article/us-facebook-cyber-idUSKCN0XV1O7

Data Protection and how to prevent Data Breaches. (2018). Retrieved from https://www.gdpr.associates/data-breach-prevention/

Evers, J. (2005). Credit card breach exposes 40 million accounts. Retrieved from https://www.cnet.com/news/credit-card-breach-exposes-40-million-accounts/

Sahadi, J. (2005). Breach affects 40M+ credit cards. Retrieved from https://money.cnn.com/2005/06/17/news/master\_card/

Sandler, R. (2018). The most common mistakes people make when choosing passwords, according to research. Retrieved from http://uk.businessinsider.com/good-best-password-2018-5

Weak passwords illegal in California from 2020. (2018). Retrieved from http://www.businesscomputingworld.co.uk/news-post/comment-weak-passwords-illegal-in-california-from-2020/

Buist, E. (2014). How to set a strong password. Retrieved from https://www.theguardian.com/technology/2014/jan/22/how-to-set-strong-password-online

Fruhlinger, J. (2018). What is phishing? How this cyber attack works and how to prevent it. Retrieved from https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Krawchenko, K. (2016). The phishing email that hacked the account of John Podesta. Retrieved from https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/

Lowry, B. (2016). KU employees fall victim to phishing scam, lose paychecks. Retrieved from https://www.kansas.com/news/local/crime/article88960532.html

Fruhlinger, J. (2018). What is phishing? How this cyber attack works and how to prevent it. Retrieved from https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

10 Tips for Phishing Prevention. (2006). Retrieved from https://biztechmagazine.com/article/2006/01/phishing-protection