Online Privacy

Name

Institution

Online Privacy

When originally designed, the online space was supposed to be a safe platform for social connections. While it still serves this purpose, it is difficult to deny that the online world is becoming increasingly dangerous. When individuals visit websites, connect on social media platforms, and consume media delivered through digital channels, they expose themselves to various harms. Having their privacy violated is among these harms. In the recent past, there have been dozens of cases where users suffer privacy breaches. Whereas these incidents are worrying, they also provide opportunities for learning. They enable individuals to learn that there are simple steps that they can take to secure their online privacy. To stay safe online, individuals need to adopt such techniques as using strong passwords, adopting two-factor authentication and limiting their online activity.

There are numerous effective strategies for bolstering one's online privacy. Among these strategies is two-factor authentication (Bogle, 2020). Basically, this security technique for securing accounts where access is only granted once an individual has presented two pieces of evidence. For example, suppose that one wishes to gain access to their school account. Leveraging the power of two-factor authentication, the system of which the account is part sends a verification message to the student's number. To gain access, the student must have the number associated with the account. This example shows that two-factor authentication limits the risk of unauthorized access. In addition to employing two-factor authentication, individuals can secure their online privacy by installing the latest updates and patches onto their devices (St. John, 2019). Usually, device makers issue updates that fix known loopholes that can be exploited to

breach privacy. Therefore, by updating their devices, users eliminate the loopholes, thereby keeping their devices and their privacy secure.

While it is crucial for users to protect their privacy whenever they are online, they should be particularly careful with their financial details. To insulate their financial information against theft, users are strongly encouraged to avoid sharing this information on such sites as shopping platforms (Forbes Technology Council, 2019). If possible, users should ensure that they do not provide personal details such as their names or addresses altogether. Most websites ask users to offer this information thereby exposing the users to elevated risk of privacy violations. Another simple technique that individuals can adopt is using strong passwords (Forbes Technology Council, 2019). While simple, this strategy plays a crucial role in limiting the threat of attacks. Passwords which combine multiple types of characters are understood to offer greater protection. Combined with the techniques already discussed above, these strategies go a long way in enhancing one's online privacy.

Even after adopting the strategies discussed above, individuals can still suffer privacy violations. To further minimize their risk, they should take charge of their privacy. Essentially, this measure involves being deliberate and aggressive in protecting one's privacy. For example, individuals can limit the permissions that they grant to their devices (St. John, 2019). An individual can say, deny their smartphone the permission to make phone calls or access their contact list. This strategy functions by eliminating opportunities that can be exploited to execute privacy breaches. Basically, for user privacy to be secure, individuals should reclaim power from technology companies which wield unacceptable level of influence and cannot be trusted to prioritize the safety and privacy of their users.

While promising and highly effective, the strategies addressed above still do not guarantee total security. Apart from these strategies, individuals should protect their online privacy through the use of virtual private networks (VPNs) (Forbes Technology Council, 2019). In the recent past, VPNs have become increasingly popular as individuals become wary of government surveillance. Basically, VPNs work by masking an individual's location (Forbes Technology Council, 2019). For example, users in countries where online activity is strictly monitored can use VPNs to hide from the authorities. Tools that block trackers are another resource that users can leverage in their quest for ultimate online privacy (Forbes Technology Council, 2019). These tools are similar to VPNs in that they insulate individuals against surveillance. For example, they frustrate such software as cookies that websites use to track and monitor user activity. Furthermore, individuals can use browsers which promise to spare no effort in guaranteeing their privacy. Such browsers as Tor are known for offering such features as encryption which minimizes the possibility of having one's privacy breached.

In closing, the importance of online privacy cannot be over-emphasized. If they truly wish to be secure online, individuals must take action. Such strategies as using strong and complex passwords and updating their devices are tremendously effective in offering privacy protection. Additionally, individuals need to minimize the amount of personal information they share. While individual action is needed, technology companies should also be involved in efforts to guarantee online privacy.

References

Bogle, A. (2020). Give yourself an online privacy check-up and start 2020 securely. *ABC.* Retrieved January 25, 2020 from https://www.abc.net.au/news/science/2020-01-20/online-privacy-checklist-passwords-two-factor-authentication-vpn/11863496

Forbes Technology Council. (2019). A beginner's guide to online privacy: 12 important tips. *Forbes.* Retrieved January 25, 2020 from https://www.forbes.com/sites/forbestechcouncil/2019/06/07/a-beginners-guide-to-online-privacy-12-important-tips/#5e4fba8b53ed

St. John, A. (2019). 5 easy ways to protect your digital privacy in 2019. *Consumer Reports.* Retrieved January 25, 2020 from https://www.consumerreports.org/privacy/ways-to-protect-digital-privacy/