Overview

After reviewing the concerns and requests from Alice and taking into consideration the personality traits and the current security holes in Mary's online activities, we have come up with two solutions to the proposed problems. They include:

- An incredibly cheap plan put together with the goal of choosing software that is cost effective while still being simple to use.
- A paid plan, which is slightly more expensive but easier to use.

We have also compiled a list of 10 rules for Mary to follow when she is online with her devices. We believe implementing the software we have recommended and following our simple ten steps, Mary will see a significant boost to her online security and Alice can rest a little easier at night.

Software Report - Budget Plan

Antivirus - *AVG*

Cost - Free

AVG Antivirus is one of a few antivirus solutions that has a completely free version to use. Most free antivirus will offer you basic computer scanning, and threat detection but we have chosen to select this particular piece of software out of all the options as it goes a little further. As well as performing basic antivirus operations, AVG's free service also actively filters your emails for malicious links or files and automatically blocks them from being downloaded which is an important feature for Mary who tends to be over trusting with what she reads online and who has a history of compromising her accounts. These features should help in reducing the amount of chances that this can happen in the future

Password manager - *Nordpass*

Cost - $1.50

Nordpass is the best value for money password manager available today, at the low cost of only $1.50 per month you get most features that are available on most password managers. Two competitors at this price range (Zoho vault and Bitwarden) are slightly cheaper at only $1.00 per month but you are giving up some key features such as, auto-filling of personal data and passwords as well as being alerted of data breaches involving your connected accounts. Because these features make management a lot more simpler, especially the auto fill options, we recommend Nordpass as a solution to password management. Using a password manager will add a significant boost of security for Mary's accounts. Not only will it generate new passwords consistently, they will also be significantly stronger than the current rotation of passwords she is using, which contain a lot of obvious personal information along with the same email for every service she accesses online.

VPN - *Proton VPN*

Cost - Free

It is not easy to find a free VPN service these days that doesn't eventually make you pay for the service after a trial period or reaching a specific data limit. One such that does remain free is Proton VPN, owned and run by the same company that offers the free encrypted email service Protonmail (more on this in a moment). Although options for connection aren't great in number, there are still three countries that you can connect to for free and the service is as good as any paid option available on the market today. Proton VPN will significantly increase Mary's security by encrypting all of her web traffic, since she often tends to connect to numerous public Wi-Fi networks when traveling around. This will greatly help minimize the attack surface against Mary.

Secure Email - *Protonmail*

Cost - Free

As well as using Protons VPN service we are recommending using their email service too. Mary should keep her gmail account for all her public facing internet activities but also create a new email to use for her more sensitive accounts such as banking. We suggest keeping this email more private and only use it for more important and secure services, this should help lower the chance, severity and impact of a serious breach if one was to happen by splitting up the access a potential attacker may have in the future as well as making it much more difficult for an attacker to find an email with worthy information to steal behind it.

2FA - *Google authenticator*

Cost - Free

Most authenticators or other types of 2FA options are free, so price isn't a factor for this security service. Besides being very simple to use,, the reason we recommend using an authenticator like google's is partly due to our clients behavior and partly due to the risks of SMS based 2fa. SMS messages are not encrypted so attackers looking to intercept messages can easily see what the contents of the message is, which is a big security hole for 2fa. The second reason is our client is very trusting and has a past of accounts being compromised, this is probably due to clicking on various links sent to her on social media and through her email. This is a key attack vector for SIM-swapping attacks which are looking to intercept security messages such as SMS 2fa. For these two reasons we recommend google's authenticator which will help minimize the attack surface against Mary and provide yet another layer of security against attackers.

Review

These services combine, offer all round security and system protection for Mary's two devices at the low cost of $1.50 per month. But there is one slight drawback, and that is that the management of all four different pieces of new software (no matter how simple they are too use) may not be as simple as is needed for Mary, and this is where we have a second option which does come at the cost of a few more dollars per month for total simplicity.

<u>Software Report - Simple plan</u>

Norton's antivirus offers a $90 per year service ($7.50 per month) which, besides the two factor authentication, includes everything Mary is looking to have in a service, such as:

- Protection from Ransomware attacks

- Anti Hacking protection

- Malware and Virus protection

- Password manager

- VPN

- 50gb of cloud back

- Email filtering

- Dark web information monitoring (Alerts you if your details appear online)

For only $6 more per month we do recommend our client chooses this option over the above free options and this is only due to extra simplicity. Everything that is needed is in one piece of software that is easily managed. We do understand that price is a main factor for Mary, but simplicity in a security system is just as, if not, more important than the security systems themselves. If a system is too hard to manage or understand, you are more likely to ignore or turn off the system altogether. For this reason alone we recommend the paid option, which in the long run, will end up being a lot cheaper than any compromise that may come from any possible attack on Mary's security due to being a little less technologically savvy.

Ten Rules for Online Security

1 - **Avoid using public Wi-Fi's.**
- If you have to use one, always turn your VPN on prior to connecting.

2 - **Never connect a device that isn't yours to your computer.**

3 - **Always use 2 Factor authentication**
- For all of your online accounts (Banking, social media, email)

4 - **Keep your antivirus and browser software up to date.**

5 - **Never click on links or download files received in your emails.**

6 - **Never respond to emails asking for personal or financial information.**
- Your bank or any other institution will never ask you for personal information through an email.

7 - **Bookmark your most used websites and visit them via your bookmarks tab or bar.**
- Especially those that relate to financial or government information.

8 - **Never use the same password for separate services/accounts.**
- Let your password manager generate and manage all of your passwords.

9 - **Never let your browser save any of your login information.**

10 - **Avoid oversharing online**
- Phone numbers, addresses, travel plans or any other personalized identification anywhere online, including social media.