Data Research Center, Life in lockdown: wash your hands and work on your digital hygiene (column), April 2020
https://www.rug.nl/cf/onderzoek-gscf/research/research-centres/dataresearchcentre/working-papers-and-insights

Life in lockdown: wash your hands *and* work on your digital hygiene

These past weeks, most of us have doubled if not tripled the amount of time we spend online. We've experienced the relief of having important meetings still go ahead, the frustration of less than stable connection, and the creativity of renewing some of our modes of teaching, learning, meeting and otherwise interacting.

All this activity also brings risks, and just as proper handwashing and less face-touching are important parts of good hygiene, we propose that there is also such a thing as digital hygiene. Here are a few practices the Data Research Centre recommends;

1. Update for data security

This is a time when you should pay attention to the little pop-ups that remind you to update. Updates often include fixes or patches for security flaws. By updating, you and your data will be less vulnerable. And because we are incredibly interconnected, your data will likely contain sensitive information about dozens if not hundreds of other people too. We wash our hands and cough in our elbow not to get ill but also to refrain from infecting others. Updating security patches is no selfish act and helps protect the privacy of those friends, family members, colleagues or even lovers that we communicate with online.

If you have the time and energy, we also highly recommend turning on two-factor authentication (also known as 2FA) for your most important (or sensitive) apps and services. Your email and most used social media are a good first step. With 2FA, you build in an extra layer of protection so that hackers can't access your account with just your passwords. Given that hundreds of millions of passwords have been leaked this can save you from a criminal taking over your gmail, facebook or instagram account. Luckily, there are sites where you can check if your email has been 'pwned'

2. Choose 'better' platforms

Many of us have turned to whatever seemed most easily available as a platform to conduct meetings, teach or otherwise exchange material to continue our activities. Given how suddenly we had to transfer virtually all our social contacts online, this is not surprising. Now that we are getting used to daily video-calls it is time to consider that what is most visible and easily available may not be the best option. For example, one of the platforms that suddenly seems to be everywhere is Zoom. Even U.K Prime Minister Boris Johnson used it to chair a Cabinet meeting and posted a picture afterwards - including the room number for everyone to see (and possibly join in). This particular platform is probably not the best option, because of the amount of privacy and data you give away when you agree to use the tool. This means forfeiting the expectation of privacy during your calls, but also giving over ownership of material you share via the online tool. Furthermore, despite claims on its website, it is not end-to-end encrypted meaning that you are exposed to hackers and 'Zoombombers'.

It can seem daunting to find the right tools and to go about evaluating how harmful their practices might be. On the other hand, as more and more of our public activities (meeting, organizing social action, teaching) need to be done virtually in this period, it's well worth thinking about how best to preserve their public status. As a rule of thumb, 'paid services' are less extractive and more respectful of property. Open source tools tend to be less aggressive in their capitalization of your data. At DRC, we recommend using Wire or Signal, as they are end-to-end encrypted and score better on privacy than platforms such as Zoom. Several good overviews exist to help you decide what is most important to you (Some software architects have started on overviews for messaging apps and collaboration platforms).

3. Limit data trails from apps

Ask yourself: does location data really need to be 'on' for this app? Part of what makes data valuable is the possibility of coupling different kinds of data (for example, the location of a mobile phone in shopping street and past purchasing history). This is why so many apps systematically collect location data. While we can imagine that for some apps, this is related to the service—think of a weather app—this is not always the case. For example, does the location from where you tweet need to be traced? Given the current calls for wholesale use of location data--without proven benefits so far--in the fight against corona, a healthy dose of data hygiene also makes sense. This is not to say that you should not willingly and consciously participate in data gathering exercises that may involve location data. Our recommendation has to do with the tendency to gather this data in the background, without justification for the service in question, without benefit to the user and without explicit agreement.

Now that you have followed these 3 steps, you have taken important steps in improving your online hygiene. And in doing so protected yourself, and your contacts, from harm. Like washing your hands and coughing in your elbow, these steps help us stay in good shape.