Digital Risk Governance: Security Strategies for the Public.

Cyber hygiene in Data Protection 101. Lite version.

Rules to keep the internet from making you sad, angry, self-obsessed, and afraid.

Safety education related to cleaning up and maintaining your digital world to resist cyber threats and online security issues.

Cyber hygiene refers to fundamental cybersecurity practices that an organization's security practitioners and users can undertake.

As you have personal hygiene practices to maintain your own health, cyber hygiene best practices help protect the health.

Most network breaches are caused by exploiting oversights in basic cyber hygiene.

You need to be able to assess its current cybersecurity state and accurately evaluate your cyber hygiene.

You need to know what’s on your network, how it’s all connected and the associated risk.

Firewalls are a first line of defense in network security by preventing unauthorized users from accessing your websites, mail servers, and other sources of information that can be accessed from the web.

+ Employ device encryption (Like FileVault Apple)

But not on smartphones, so:

Update your apps, web browsers, and operating systems regularly to ensure you’re working with the latest programs that have eliminated or patched possible glitches.
Setting up this feature to update automatically will help ensure you have the latest protections.
These updates are particularly important because they often include software patches.

Software developers issue security patches whenever they discover software flaws that could let in viruses or hackers.

Developers may not always alert you when a critical patch has been implemented, because this might give hackers the heads-up, as well.

Review privacy and security settings on accounts and social media.

Your apps and accounts are sucking up a surprising amount of data on you, but you often have some amount of control over that just not by default.

Generally, the less data you make available to the internet, the better.

Some applications will make important personal data like your email address, birthday, and location available publicly.

Unless you have a good reason for making those available, you should look for privacy and security settings that allow you to hide critical information from the public + please, check all the options about security (not only by the apps but, by asking on the web, too, for more about)

Two-factor or multi-factor authentication is a best practice that offers an additional layer of protection.

Two-factor authentication usually requires you to submit your password and username along with, say, a unique code that is sent to your cell phone.

Also, make sure your router offers WPA2 or WPA3 encryption to maintain the highest level of privacy of information sent via your network.

Pdf complement to N° 93
Infos arttrustonline.com/artwork/307911

I created a poster available for teenagers or anyone who wishes to display.

Please ask the original file. It is free :)

It comes with a list of things to pass on.

In my sense, after a meticulous study, it is really necessary.

+ A magazine very complete will be available at the end of August.

A lite version is already available and the poster will come with mag version 2.

+ additional information related to the poster in progress.

ussignal.com/uploads/general/Documents/General/Ebooks/Data-Protection-101-ebook.pdf

books.google.fr/books?id=yB8SEAAAQBAJ&lpg=PA123&dq

youtube.com/watch?v=GWJnxAm90rc

Take smart decisions on your smart devices.

Call on me to help and, stay safe online.

You can download this pdf + share.

19 August 2021. Veronicaindream.space