HealthManagement.org
Promoting Management and Leadership

Your GDPR Responsibility: tips & tricks

Mag. Christian Marolt
Executive Director &
HealthManagement
******@***marolt.com

Secretary General - European
Association of Healthcare IT
Managers - HITM
Executive Director -
HealthManagement(dot)org

LinkedIn Twitter Facebook

Yes this is yet another notice about GDPR, but read on for advice about online safety management.

The most robust laws and regulations won't protect you if you are not extremely careful about your personal online safety. Here are our top tips to be safe online.

Be careful with unknown or questionable sources

Always check the sender email and the real domain you are (re)directed to if you click on a link in an email. If there are any differences **RED ALERT!** Stop and leave.

I got an invitation from mılka.com, the chocolate makers - very tempting!. At first I did not notice a small

alteration in the i. Just in time I noticed this was a scam and reported it. Within the shortest time the site was offline.

Always check the from email and description. When an email claims to be from CM – HealthManagement the email should reflect this: cm@healthmanagement.org. If the sender email shows asdaölja@gmail.com be careful, and double check if this is genuine.

The bank or tax office never ask you to confirm your data or send confidential information via email. If you are on a website (paypal, a bank, etc) ensure that you land on a real, genuine website. Check if you have a secure connection (https) and if the certificate is matching the url.

Some scammers sent from my private email reminders about tax credit. Not only did I receive thousands of bounced messages, I was even more astonished when I got hundreds of answers which could have made me a rich man.

Come on, c@marolt.com is surely not an official email of the UK Inland Revenue. Applying basic common sense would have avoided risk and danger.

Password hygiene

Take your password hygiene seriously! This is the easiest way to avoid trouble and scams. Any social or easy password can be hacked quickly.

Social passwords are passwords with personal referral anchors. Say you have a son called Joseph and his birthday is 3 October 2010. Using Joseph031010 would be easy to guess and should never be used.

Easy passwords have fewer than 8 characters with no special characters or numbers.

Imagine I hack one of your email accounts. Within a short time I can reset all passwords linked to this email and gain valuable access to most of your personal online life.

Remedy:

The only way out is to start using a very long password, at least 20 characters, and change it for each account and device.

You may fear, how can I ever remember this? Simple!

Step 1: Take a basic phrase, ideally something you have wonderful memories of.

Example: Cyprus is a great holiday destination

Step 2:
Alter this phrase as much as possible so that you can still remember it.

∫: C%prUSis$Gr8H§LL$dayDeST$NAtion

Step 3:
Now establish a pattern to use this basic phrase for all your passwords but make it unique for each of your particular accounts.

Sample Facebook:

FBC%prUSis$Gr8H§LL$dayDeST$NAtion or
C%prUSis$Gr8H§LL$dayDeST$NAtionFB or
FC%prUSis$Gr8H§LL$dayDeST$NAtionB or
C%prUSis$Gr8H§LFBL$dayDeST$NAtion

With such a high-standard password even the best hacking technology will be frustrated and fail.

Step 4:
Sharing is in this context not caring but dangerous

Step 5:
Change it regularly! Even though this password is strong, change it at least once per year and ideally more often.

Get your own, private email address

Imagine, today you are with Telenet, tomorrow with speed24, then one day with cablenet. Your email will change according to the service provider. Not a smart move if you would like to stay in touch with people.

Now, some people turned to Gmail, Hotmail or other competitors in order to have the same email address even with provider change. You may ask, is this any better?

Bluntly NO! Avoid public emails service providers as they spam you with ads and secretly spy on you. With AI technology they combine your browsing habits, emails, event participation and address book to map a dangerous picture of your personality and privacy.

Get your own domain!

For peanuts you can get your own domain. And then for a little more money you can get yourself a serious internet host. With this you can increase your internet security and independence.

The domain I normally use is Marolt.com. Now, as there have been constantly people contacting me to buy this domain from as I did not have a website (some do not understand that your domain is great even if you use it only for emails) I put up a dummy site.

Then all my family members and even third parties with the same surname have been extremely grateful to have their own dedicated email address.

Don't you agree that it is cooler to have c@marolt.com or Christian@marolt.com as your email instead of maroltchristian@telenet.be or chirstianmarolt147@gmail.com?

The key advantage is that when I sign up somewhere I am able to put though a catchall account any email into this system. With facebook I have facebook@marolt.com, with google it is google@maroltcom and so on.

Recently I got more and more spam emails to facebook@marolt.com. That means either there was a hack or the Zuckerbergs made some cash out of my data. How would I have ever known this without my dedicated email assignment policy?

GDPR update

Now please let me direct your attention to the GDPR updates.

Who are we?

ICU Management & Practice and HealthManagement.org are brands of MindByte Communication, a worldwide communications agency. We promote management, leadership and cross-collaboration in healthcare. Our main base is in Limassol, Cyprus and we have representations in Belgium, Bulgaria, Canada, UAE, India and Pakistan.

How do we collect your data?

Being the dedicated communications channel of different associations such as the European Association of Hospital Managers, European Association of Healthcare IT Managers, European Health Management Association, BIR, and many more, contractual partners and their paying members have free access to our platform. This means either we have received those personal data from them as part of our agreement in order to fulfil our contractual obligations (The bare minimum is an email address and your affiliation) or they have encouraged you to sign up with us. We always requested double opt-in.

Several congresses like to partner with us and provide a full years' access to their congress advantages.

If you attend this congress and pay your congress fee, a subscription to our platform is part of the benefits you get. In this context we may hold your data as you consented by paying your congress fee.

What will change for you?

In reality almost nothing. Already before the GDPR implementation we have administered the most prudent and strict personal data policy. We have always only kept the bare minimum of data about you. These data are stored, fully encrypted, on our own dedicated, professionally managed servers. They are equipped with the latest security tools. Furthermore, we use as well CDN networks to further protect your data.

Applied changes:

- **Unsubscribe**: the new form is that you can unsubscribe by either pressing a link or sending an email request. We do the rest for you.
- **Privacy Policy**: we have made it even more simple for you to understand this policy. Click here to read it
- **Cookie Policy**: Click here to read it
- We will continue sending you our journal and/or newsletters. You can update your preferences in your personal lounge on our website or opt-out at any time.

Published on : Wed, 23 May 2018