IKF Michael Janssens & Gertrude de Vries

Disclaimer

This booklet, *Online Safety*, has been prepared as a general guide for volunteers of the International Korfball Federation during their international travels. The information provided is based on the best knowledge and intent of the authors at the time of writing. However, it may not be complete, entirely up to date, or applicable in all situations.

No rights can be derived from the contents of this booklet. The authors and the International Korfball Federation accept no responsibility or liability for any inaccuracies, omissions, or the consequences of any actions taken based on the information provided herein.

This publication is protected by copyright and may not be copied, distributed, or used for commercial purposes without the prior written consent of the authors.

© 2025 The authors. All rights reserved.

Why did we write a booklet?

With the upcoming World Games, and many other international tournaments and events on the horizon, volunteers of the International Korfball Federation are increasingly active across the globe. As we travel and represent the IKF in various countries, we also interact more frequently with digital tools, platforms, and networks. At the same time, the online world continues to evolve rapidly—bringing not only new opportunities but also new risks.

Cybercrime and digital threats are constantly changing. What was considered safe yesterday may no longer be secure today. That's why it is essential to regularly update our understanding of online safety and digital best practices.

This booklet aims to provide practical guidance to help you navigate the online world more securely while fulfilling your volunteer tasks both at home and when travelling. Protecting your personal data, securing your devices, and being aware of potential cyber threats is not only important for your own safety but also for safeguarding the reputation and digital infrastructure of the International Korfball Federation. We also want to help you understand why certain measures are important, rather than just focusing which rules to follow.

We expect to update this booklet in the coming years when new technologies and threats may evolve. We welcome your feedback and knowledge to make this booklet as accurate and up to date as possible.
Let's work together to ensure a safe and secure digital experience—for yourself, for your fellow volunteers, and for the entire IKF community.

Gertrude de Vries, Chair IKF Media

Who are we?

Michael Janssens – Chair IKF ICT, IKF Jury member.
I have been working as a train driver at Belgian Railways (NMBS) for 8 years, ensuring the safe and smooth transportation of passengers throughout the country. Besides my career in public transport, I have a strong passion for computers and technology. I have been active since 2012 in the IKF (International Korfball Federation) IT committee, serving in various roles as jury member and chair, and for the past 2 years as IT manager. I also have a passion for multimedia and photography, applying my knowledge to contribute wherever needed. Currently, I'm attending evening school as a system and network administrator to further expand my technical expertise.

Gertrude de Vries – Chair IKF Media, IKF photographer.

In daily life I am a teacher to 16 - 60+ year olds at a medical school for nurses and assistants. I teach pathology and other medical topics, but also other things like Ethics, Administration and ICT. Teaching my students how to stay safe online and how to keep patient data confidential is part of my job.
My hobby, that became my second job, is photography. I am also the Secretary General of Korfbalfoto. A club were photographers that like to shoot korfball come together and share expertise. Since one year I am the chair of the IKF Media committee and the secretary of the IKF Volunteer and Fan committee. Next to that I am the media liaison for the Extended Events and Learning Academy committee.

Summary

🔐 Before You Travel

- **Use a clean device** – factory reset or new phone/laptop.
- **Log out** of all accounts (Gmail, Facebook, banking, etc.).
- **Remove personal data** – photos, documents, passwords.
- **Install:**
  - A **paid VPN** (with kill switch)
  - A **virus scanner** (also for phones)
  - An **eSIM** for affordable internet (check if your phone supports it)
- **Update** your system and apps.
- **Create a new email account** just for your trip.
- **Use two-factor authentication** for all logins.
- **Print** tickets, maps, and key info (don't rely only on your device).
- **Pack your own charger and power bank** (never use public USB ports).

🌍 While Travelling

- **Avoid public Wi-Fi** (airports, hotels, cafés) – always use your VPN.
- **Turn off auto-connect** to Wi-Fi and Bluetooth.
- **Lock your device** with a strong password or fingerprint.
- **Never leave devices unattended.**
- **Don't plug in USB sticks** or unknown chargers.
- **Be careful with QR codes** and strange links.
- **Use mobile data** from your eSIM instead of Wi-Fi.
- **Don't log into important accounts** unless necessary.
- **Think before posting** on social media (use a temporary account if needed).
- **Don't share your device** with others.

🏠 After Returning Home

- **Don’t connect your travel device** to other devices.
- **Log out** of all accounts from a safe device.
- **Change all passwords**.
- **Run a virus scan** on your travel device.
- **Check for strange activity** in your accounts.
- **Use “Have I Been Pwned”** to check if your data was breached.

⚠️ Common Threats to Avoid

- **Public USB charging ports** (risk: “juice jacking”)
- **Free Wi-Fi** (risk: spying or fake networks)
- **Fake QR codes or links** (can install malware)
- **Apps from unknown sources** (only use official app stores)
- **People asking to borrow your device** (they may steal info or install spyware)

🧠 Remember

- Even if you think "I’m not interesting," your **data may still be useful** to criminals.
- Online safety protects **you**, the **IKF**, and **your teammates**.
- Ask IKF ICT if you have **questions or concerns**.

Understanding Online Risk

Online risk is not something that can be measured in exact numbers or clearly defined for everyone. It is not the same for all people, and it is not simply “safe” or “unsafe.” Instead, online risk works more like a sliding scale—it changes depending on many different things. For example, your personal online risk can depend on:

- Your background – People with different levels of digital knowledge may face different risks. What’s your job? Which people are you connected to and do they hold important positions?
- Your role or function for the IKF – Someone handling sensitive information or communication may be a bigger target for cyber threats.
- The devices you bring – A personal phone may be more secure than a shared laptop, or vice versa, depending on how they are protected.
- The apps or platforms you use – Logging into email, social media, or file-sharing systems may expose you to different risks.
- The country you live in or travel to.

Because of all these factors, it’s important to think about your situation and take steps that fit your level of risk. What works for one volunteer might not be enough for another.

Should I be scared?

Let’s keep seeing things in perspective. Online dangers are everywhere, also at home when you’re not travelling. Let’s be sensible and aware. If you are worried, come talk to one of us and ask your questions. Hopefully after reading this guide, you will feel more able and confident to handle obscure situations.

Smart Travel Tech: What You NEED Abroad

VPN • eSIM • Virus Scanner
Stay connected. Stay safe. Save money.

🌐 VPN (Virtual Private Network)

✅ What it DOES:

- Hides your location online
- Scrambles your data on public Wi-Fi
- Lets you access apps & websites from home

❌ What it DOES NOT do:

- Does *not* remove viruses
- Does *not* block bad apps or downloads
- Is *not* a replacement for antivirus software

🛡️ Why you need it:

Public Wi-Fi at hotels, airports, venues and cafes is risky. A VPN protects your personal info from hackers by scrambling it.

📱 eSIM (Embedded SIM Card)

✅ What it DOES:

- Gives you a local data plan without buying a SIM card
- Lets you switch easily between home and travel numbers
- Saves you money on roaming fees

❌ What it DOES NOT do:

- Does *not* protect you from viruses or spying
- Does *not* secure your Wi-Fi or internet use
- Is *not* supported by all phones (check first!)

📶 Why you need it:

Stay online affordably and avoid huge phone bills abroad.

Smart Travel Tech: What You NEED Abroad

VPN • eSIM • Virus Scanner
Stay connected. Stay safe. Save money.

🛡️ Virus Scanner (Antivirus App)

✅ What it DOES:

- Scans your device for viruses & malware
- Warns you about dangerous apps or files
- Keeps your phone running safely

❌ What it DOES NOT do:

- Does *not* secure your Wi-Fi (that's a VPN's job)
- Does *not* unblock websites or apps abroad
- Won't lower data costs

🔒 Why you need it:

Traveling often means using new networks and apps. A virus scanner keeps your device safe.

✅ Use All 3 for the Best Travel Protection

Tool	What It Does	What It Doesn't Do
VPN	Safe, private internet on public Wi-Fi	No virus protection
eSIM	Affordable mobile data while abroad	No digital security or virus protection
Virus Scanner	Stops malware & keeps your device clean	Doesn't hide your activity or lower data costs

---

✈️ Travel Smart, Stay Safe

Bring **all three tools** with you:

- **VPN** for secure internet
- **eSIM** for cheap local data
- **Virus Scanner** for device protection

🛡️📱🌍 Safe travels!

In case of high risk travel destinations:

Question 1: Do you really need to bring your phone or device?

- **Consider going old school off line**. Using a notebook and pen for countries that are considered high risk when it comes to online safety
- Some apps like Google Maps, WhatsApp, Gmail etc. will not work in some countries unless you will be taking extra measures (VPN).
- Only take what you REALLY need.

"I am not an interesting target."-

Maybe not, BUT you might become an interesting target in the future. Information can be used to manipulate you when you're, for example, in an interesting position at a company. And for many companies and organisations data about you is very interesting. It makes it easier to approach you in a way that seems familiar to you.
How many steps/ connections are you removed from someone in your address book that is in a top function at a global company or organisation?

What can you do?

1. **LOW-LEVEL: LOG OUT of all your accounts**. Even Google/Gmail, Fitbit, Facebook, Instagram, Twitter, Tiktok, Snapchat, IKF, Paypal, Banking app, games (sometimes connected to Meta account), etc.
   Don't share your device with others, lock the screen, don't leave it unattended, **don't plug it in** any USB ports, other than the one on your own charger. And buy a **good VPN with a virusscanner** included, also for your phone. **Don't use Wi-Fi**

2. **HIGH-LEVEL: LEAVE your phone at home. Travel with a burner phone** with minimal apps and data on it. Create a **new number**, create a **"travel only" email address**, don't log in to any accounts (how tempting it might be), don't put any telephone numbers in your contact list. Don't connect to anything: no Wi-Fi, no USB ports, no banking account, no Google, nothing. **After the trip "burn" the phone** and don't use it anymore. Change all your passwords on your device that stayed at home. Destroy the burner phone/laptop/USB-sticks. Use a **VPN and virusscanner of high quality**.
   We will break down the steps in this document later

Question 2: Do you need connection to the internet?

- Stay off line. If your device can function without being connected to the internet, that would be much safer.
- Entertainment: maybe you don't really need to watch things on your own device but can watch tv or read a book
- Travel information and flight tickets can be printed instead of being stored on your device, you can print your itinerary or notes at home or write things down
- Do you need to transfer data/photos/videos to other team members online, or can it wait till you are at home or maybe through other pathways?

Unsafe Wi-Fi "Man-in-the-middle-attack"-

Public Wi-Fi networks (like in hotels , cafés or sport venues) can be faked, monitored or hacked. Anyone can watch what you do online and steal login details or personal data, or maybe even put a script on your device, by having you click on "agreeing to conditions" or install a "program needed for the connection".
Consider all internet traffic heavily monitored and recorded for later, Even when it's encrypted. With new AI techniques and quantum computing on the horizon, it will only be a matter of time until the code is cracked.

What can you do?

- **Never go on local Wi-Fi**. **Never**. Not even when it is very tempting because you want internet access fast and other things do not seem to be working. Just be patient and wait. Wi-Fi is not safe. Anyone can create a Wi-Fi point (and make it look legitimate) and control, store or copy the data through that Wi-Fi network.
- **Buy a good VPN**. Pay for one. Don't be too cheap and settle for less quality and safety using a free one. Use one with a kill switch when the VPN disconnects (like NordVPN) so you don't go accidently online when it disconnects
- **Buy a good Virus Scanner**. Yes, also for your phone. The app store security is not sufficient enough.
- Turn off automatic back ups and maybe even automatic updates
- Don't connect to other devices (turn off Blue tooth etc)
- **Turn off auto connect** to Wi-Fi etc
- **Use your 4/5G data from your E-sim**

Question 3: What's on your phone or laptop?

- Think carefully what information is on your phone/device:
- Contacts: telephone numbers, addresses, birthdays, email addresses, family connection
- Locations where you have been: workplace, places visited, home address, public Wi-Fi you connected to
- Search history
- Visited websites, including the naughty ones
- Many apps that know a lot about you: vitals, tracking (Fitbit, Strava, Social media, etc) Also think about dating apps, cloud storage
- Password management, autocomplete functionality
- Stored documents or images, also private images, also think about cloud storage
- Details from work or IKF, medical information
- Chat history
- Social media activity (including your opinions, private life)
- History of purchases online, client loyalty details
- Your connections to people: who are your friends, who is your boss?
- Music (Spotify), film (Streaming services), food, beverages or substances (ordered online) or other preferences, including sexual preference if you visited certain websites or dating apps
- Details about your religion

So all in all that is a lot of interesting data about you. What are you ready to share? And what could get you into trouble in certain countries?

"I have nothing to hide."- Yes, you do. You might not have many secrets but you DON'T want people to know your passwords, codes, address, medical records or other sensitive information. You actually have a lot to hide for people that have no business knowing these things about you. The more they know about you, the easier it is to make a fake claim that seems legitimate because it has so many accurate details in it.
In certain countries your online activity can get you into trouble. Think sexual preference, religion or consumption or use of certain substances.

What can you do?

- **Bring a clean, new, unused phone or device**, or one that has been set back to factory settings and has **no history** in it.
- **Don't log into your usual accounts** like Google or email, create a new, unused account and email address
- **Clean** your history thoroughly
- **Log out** of as many apps and accounts as possible
- **Especially LOG OUT of your password manager**
- Basically be a complete new person online

Question 4: How do you use your device?

How do you use your device? Are you glued to it, constantly checking all kinds of data? Do you have FOMO (Fear Of Missing Out) if you have to disconnect for a while? Do you feel the need to constantly share where you are, sending photos, posting Instagram worthy pictures and stories? Do you want to continuously talk to your friends and family? Or maybe because of your function you need to connect with the internet and work online a lot?
These kinds of behaviours make you more vulnerable online because you are heavily dependent on internet connection and most probably do not tolerate being disconnected for a while.
Do you charge your phone through unfamiliar USB-ports (because you can't run out of battery), do you connect to free Wi-Fi (to spare costs)?
Nothing wrong with that (well apart from the free Wi-Fi), but it is good to be aware of the risks.

"It's too much trouble, too much work."- Yes it is a lot of work, and that's what phishers, hackers and other ill meaning groups count on. That you don't want to go through all the trouble, and out of convenience or ignorance take very little precautions. In this case you really would rather be safe than sorry.
Our ICT specialists can help if you are feeling overwhelmed or concerned. The safety of you as volunteer but also for IKF as an organisation is very important.

What can you do?

- Bring your own charger and don't plug into any USB-ports. Never.
- Bring your own power bank
- Consider sharing your travels on a temporary social profile or a website (not an app) like Polarsteps.
- If not a temporary profile: scan your profiles for sensitive information or photos (could be as simple as a pride flag) and change your password immediately (on a device that stayed at home) when home and log out of all other locations/log ins.
- Keep your device with you, don't leave it unattended
- Always keep your device 'locked'
- Don't connect with other devices or tv's etc. Turn off Bluetooth, NFC, Data transfer through cable etc.
- Only connect through your personal 4G/5G data. Not Wi-Fi
- **Don't put any USB-sticks** in your device
- Have as few apps installed as possible, don't install dodgy apps. Even if they are in the app store. That's not 100% guaranteed to be safe.
- Work with websites that have http**s**:// in front of their web address. The **s** is important, it means they are safe. And check their certificates.
- Don't scan QR codes. If you do, check thoroughly what web address they send you to and check the safety. Don't fall for the convenience trap.

Question 5: How seriously do you take online safety?

Are you a person that clicks down the menu to deny all optional cookies? Do you update your device regularly? Do read what you are actually agreeing to when they ask you to accept the terms of agreement? Do you leave your device unattended? Do you lock your screen? Do you use safe passwords or the name of your first pet with your birthyear added to it and do you use it for everything? Do you install apps without checking if they are safe? Do you download stuff? Do you scan QR codes and click on links without checking? Do you actually check if the sender of the email is a legitimate party and is who he says he is? Do you accept all friends requests on social media and share your details with everyone? Do you go into privacy settings of your apps and select what information you want to share? Do you connect to public Wi-Fi?

As you can see we could probably fill a year long course with this. There is so much to say and so much people probably do not understand the risks of.

We have to find the middle way between 'top spy security agent' safe and 'completely ignorant idiot' unsafe.

"I don't really care."- Sorry, but it is not only about you. YOU might actually be the key to getting other targets. The data you store in your phone, like numbers and birthdays, addresses, even photos that show what people look like, can be used to get to others, also the ones that are dear to you. Vulnerable people in your surroundings could get phishing messages using details that come from your data. You can be the access to the organisation for hackers, where everyone else was careful.

In two steps you could be connected to someone leading a big international company. If you log in unsafely into the programs or websites of an organisation, you compromise the safety of the whole organisation. This also means the safety of IKF and other IKF volunteers can be compromised.

What can you do?

- **Keep yourself informed and educated**. The more you know, the less likely you will be a victim. Make sure you understand WHY some measures are taken instead of just following a rule.
- Make sure the devices and apps you have installed are **updated** to the newest version
- Have **unique and secure passwords**
- **Lock** your devices with passwords and biometrics (like fingerprint)
- Don't leave your devices unattended
- **ALWAYS check before you click** on links, QR codes etc.
- Check what kind of permissions you give apps on your phone. Install as few apps as possible and set up privacy settings to protect your data.
- Don't download apps from websites, only from the official app stores, and even then be careful and check reviews
- **Don't click on links in emails and messages**. Always research if the message is a message from who you think it is and check their website. When in doubt, contact them through the official channels, not through the same message system that sent you the original message.
- Be aware when something is "too good to be true" or "too easy".
- Don't log into IKF accounts or other accounts unless necessary
- Use **two factor identification** for all processes/ log ins
- Leave devices at home when not necessary

CHECKLIST (use to your own discretion depending on the level of risk that is involved with the country you are travelling to)

Before leaving

- ☐ Leave your devices at home if possible
- ☐ Arrange a burner phone and/or laptop OR prepare your regular phone. If you use an old phone, put it back to factory settings and erase all old data
- ☐ Make sure your devices are updated with the latest version of the operating system software
- ☐ Make sure apps are updated
- ☐ Remove apps that are not necessary or could be compromising
- ☐ Arrange for a **good VPN** for all devices
- ☐ Arrange for a **good virus scanner** for all devices, including your phone, make sure you update it
- ☐ Purchase an **E-sim** with enough data to stay online
- ☐ Create a new, separate email account for new accounts with no history
- ☐ Only add the important numbers/contacts to your phone
- ☐ Install **two factor authentication** and test if it works
- ☐ Remove search history and visited websites, maybe even remove bookmarked websites if they can be an issue
- ☐ Remove sensitive data like documents and photos
- ☐ Research which topics are considered sensitive in the country you are travelling to, so you don't offend anyone by mistake and don't break any laws or rules without knowing it. Show respect for your host
- ☐ Consider emptying your contacts list
- ☐ Log out of all accounts that are not necessary, especially the apps that contain a lot of personal and possibly compromising information and banking apps
- ☐ Bring your charger
- ☐ Bring a power bank
- ☐ Bring your own charging cord
- ☐ Bring your own USB sticks if needed
- ☐ Lock your devices with password and biometrics
- ☐ Print documents on paper
- ☐ Take a notebook and pen with you
- ☐ Print your tickets and travel information
- ☐ Write down contact information and other important information, maybe even scrambled or in code
- ☐ Consider having a trusted person at home that can access and monitor your accounts
- ☐ Check which apps or services are blocked in the country that you are going to
- ☐ Look for trustworthy apps and services as alternatives

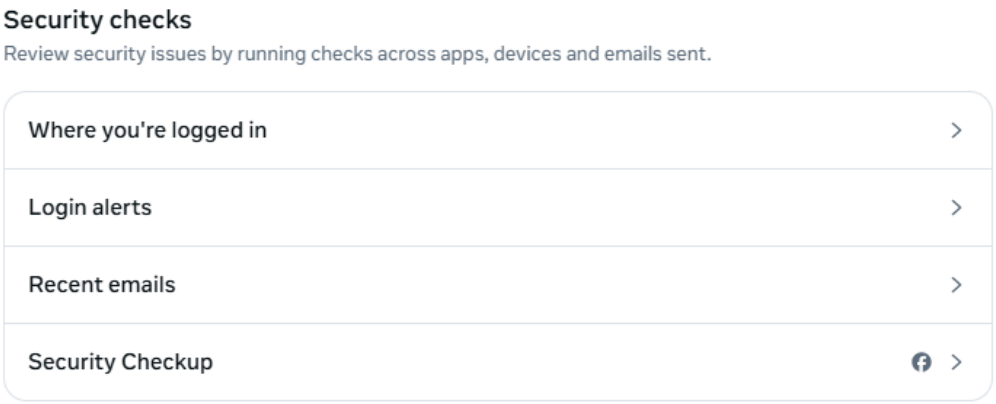
When travelling and on site

- ☐ Be prepared to have your devices searched at customs or at other moments
- ☐ Bring your power bank and original charger on the plane and to the airport, only charge through electrical outlets and **not through USB ports**

- ☐ **Don’t use airport, venue and hotel Wi-Fi**
- ☐ Turn off auto-connect to Wi-Fi
- ☐ When they take your phone or device at customs and bring it back to you later, be aware that the possibility of spyware being installed on it, is very real
- ☐ Have printed tickets and travelling information ready
- ☐ Be careful with QR codes
- ☐ Connect to as few devices and networks as possible
- ☐ If you need to share, use websites like WeTransfer
- ☐ Don’t log into IKF websites unless absolutely necessary
- ☐ Use two factor authentication
- ☐ Be aware that everything can be monitored and stored, also the use of local apps
- ☐ Stay away from illegal or sensitive activities online or off line, be aware of sensitivities in the country you’re travelling to
- ☐ Post the photos you want to keep to a temporary social media account or to a website like Polarsteps

When arriving back home

- ☐ Keep your device offline when arriving home
- ☐ Take a safe device that stayed at home and use it to log all your accounts out of all other locations
- ☐ Then change the password of the account to a new password
- ☐ Don’t connect to any devices that have been on the trip
- ☐ Don’t use any USB sticks or external hard drives that have been on the trip
- ☐ See everything that has been on the trip as “contaminated”
- ☐ Visit Polarsteps and the temporary social media account as a guest and download the photos you posted there, or take screenshots to keep those moments
- ☐ Regularly check if your data has been in a data breach at the website of ‘Have I been Pwned’.
- ☐ Monitor and check your devices and accounts and don’t ignore strange events. Run a virus scanner regularly
- ☐ Regularly check where your accounts are logged in. If you see any suspicious activity, log all devices out and change your password



Example of Meta's Account centre

How can I tell that I have been infected with spyware or malware?

You can't tell in most cases. It is usually invisible to the owner of the device or account. You could maybe notice your device getting very slow or not reacting or turning itself on and off at weird moments or getting overheated. Sometimes the device notifies you that the internal storage is full or it is otherwise behaving strangely.
You can run an extra virus scanner to see if it can find anything, but if it doesn't, there can still be some undetectable malware or spyware.
You can try to set the device back to factory settings, but even that might not be enough to clear all the malware or spyware from your device. Consider your device compromised. And stay away from connecting to other devices. You don't want to contaminate others.

Some Common Methods Criminals Use

(Cyber)criminals have many tricks to try to steal information or access your devices. As a traveling volunteer, it's important to know these methods so you can spot and avoid them. Here are some of the most common ones:

🛡️ Common Cyber Threats and How to Stay Safe

Threat	What It Is	How to Stay Safe
🔌 **Juice Jacking**	Malware or data theft through public USB charging stations.	- Use your own charger & wall socket - Use a USB data blocker
📶 **Unsafe Wi-Fi**	Hackers watch or intercept data on public networks.	- Avoid logging into sensitive accounts - Use a VPN - Turn off auto-connect
💻 **Malicious Scripts**	Dangerous links or QR codes that install malware or steal data.	- Don't click unknown links - Be careful with QR codes - Check links first
⌨️ **Keyloggers**	Software or devices that record everything you type, including passwords	- Avoid public/shared computers - Use antivirus software - Update your system
🦆 **Rubber Ducky USB**	Fake USB sticks that act like keyboards and run harmful commands.	- Don't plug in unknown USB devices - Lock your laptop when not in use
📱 **App Exploits**	Outdated apps or systems with security holes.	- Keep apps and system updated - Download only from official app stores

Also consider ‘old school’: looking into your device. People that have no business using your device, may try to look what’s on it. It only takes a little time. They can copy things off your device or install malware on your device for them to monitor you and use later from a distance. In some countries authorities might ask you to open your device at the airport or at other locations.
How to stay safe: Lock your device with passwords and biometrics. Don’t leave your device unattended. ‘Clean’ your device before your trip. Remove everything that is not needed for your trip. Remove also everything that is sensitive. Log out of all accounts. If the device has been taken away from you, consider it to be compromised.

“This feels like overdoing it.” – It can feel like that because it is a lot of work and we often are not very motivated to take all precautions. But you cannot know how much risk will be involved for you personally or for the people around you. Different countries and situations have different online security threats.
Everyone should take his/her own decision in this. But let’s at least take an informed decision.