



TOURNONS LA PAGE

Pour l'alternance démocratique
en Afrique

RISK PREVENTION FOR HUMAN RIGHTS DEFENDERS

Training Session 1:

Assess risks, analyze threats and develop a security plan



WELCOME



OPENING CIRCLE

Presentation (first name, organization)

What is your dream holiday destination?

AGENDA

- **Theory and practice**
 - Introduction of concepts (threats, risks, vulnerabilities, capabilities)
 - Presentation of the security plan
 - Case study
 - Implementation of the security plan
- **Safety of Women Human Rights Defenders**
 - Specific security needs
 - Sexual violence
- **Digital security**
 - The dangers of the internet
 - E-reputation
 - Account security

THE SECURITY PLAN

What is it for?

Who has one? Who has already made one?

Presentation of a security plan template

THE STEPS OF THE SECURITY PLAN

STEP 1

Risk assessment

STEP 2

Risk matrix

STEP 3

Development of an action plan

STEP 4

Day-to-day security management

STEP 1 - RISK ASSESSMENT

1.1. ANALYSIS

Need to analyze :

- Economic, political, military and social contexts
- Outlook for the future
- Global context security
- Forces involved (= any person, group or institution playing a role in the context)
 - favourable to your activities, which can be supportive
 - opposed to your activities, which can be the source of security problems
- Stakeholders (= any person, group or institution having an interest in or being involved in the outcome of a protection policy)
 - Interests
 - Relationships between them
 - Influence of your activities on their interests

1.2 RISK ASSESSMENT

➤ DEFINITIONS

RISK: the possibility of an event that results in harm

THREAT: a statement or indication of an intention to inflict harm, punishment or injury (forthcoming or immediate).

In parallel there may be **security incidents**, i.e. events that may indicate or lead to a threat

➤ **EXERCISE 1:** (Poll) Vote on whether the situation presented is more of a risk or a threat.

Situation 1 - In 2010, Damien was working at Human Rights Watch, co-authoring a report on corruption in Haiti. His house shook heavily, as did all the houses in his neighborhood, before collapsing:



Risk or threat?

Correction: Damien's house was destroyed as a result of the terrible earthquake in Haiti in 2010. This disaster destroyed up to 90% of cities at times and had nothing to do with Damien personally. Damien faced a **risk**.

Situation 2 - Anne is a journalist who recently wrote an article about water pollution by a multinational company. She opened her letterbox this morning and found a folded piece of paper with letters cut out of newspapers stuck to it:



Risk or threat?

Correction: Anne is being intimidated directly. These are **threats**.

Situation 3 - Carl is a project officer at Amnesty international. On his way home from work, he parks his car on the street. The next day, as he is about to go to work, he notices that his car window has been broken:



Risk or threat?

Correction: There is no indication that Carl's car was specifically targeted. It is a **risk to** have your car broken into when you park it on the street. However, if this kind of event is not isolated in Carl's life it should be considered that it could indicate a threat (= **security incident**).

➤ DEFINITIONS

CAPACITY: any resource (including skills and contacts) that enhances safety. With regard to a risk, a distinction must be made between :

- **Existing capacities**: i.e. the resources available that can be mobilized immediately to reduce the risk.
- **Required capacities**: i.e., the resources to be acquired to reduce the risk.

VULNERABILITY: Any factor that makes it more likely or more important that a harm will occur.

➤ **EXERCISE 2:** (Poll) Vote on whether the situation presented is one of ability or vulnerability.

1- Damien lives on a seismic fault. **Vulnerability or capacity?**

Correction: This is a **vulnerability**. The risk of earthquakes is greater in seismic regions.

2- Anne's contact information (address, phone number) is secret. **Vulnerability or capacity?**

Correction: This is a **capacity**. It is harder to find Anne to threaten or harm her.

3- Carl's car is equipped with an alarm. **Vulnerability or capacity?**

Correction: This is a **capacity**. The car's alarm goes off when someone tries to steal it, alerting neighbors and Carl.

➤ PRESENTATION OF THE RISK FORMULA

In order to assess the risks, it is necessary to identify and analyse these parameters: Threats, vulnerabilities and capacities.

$$\text{RISK} = \frac{\text{THREATS} \times \text{VULNERABILITIES}}{\text{CAPACITIES}}$$



=



X



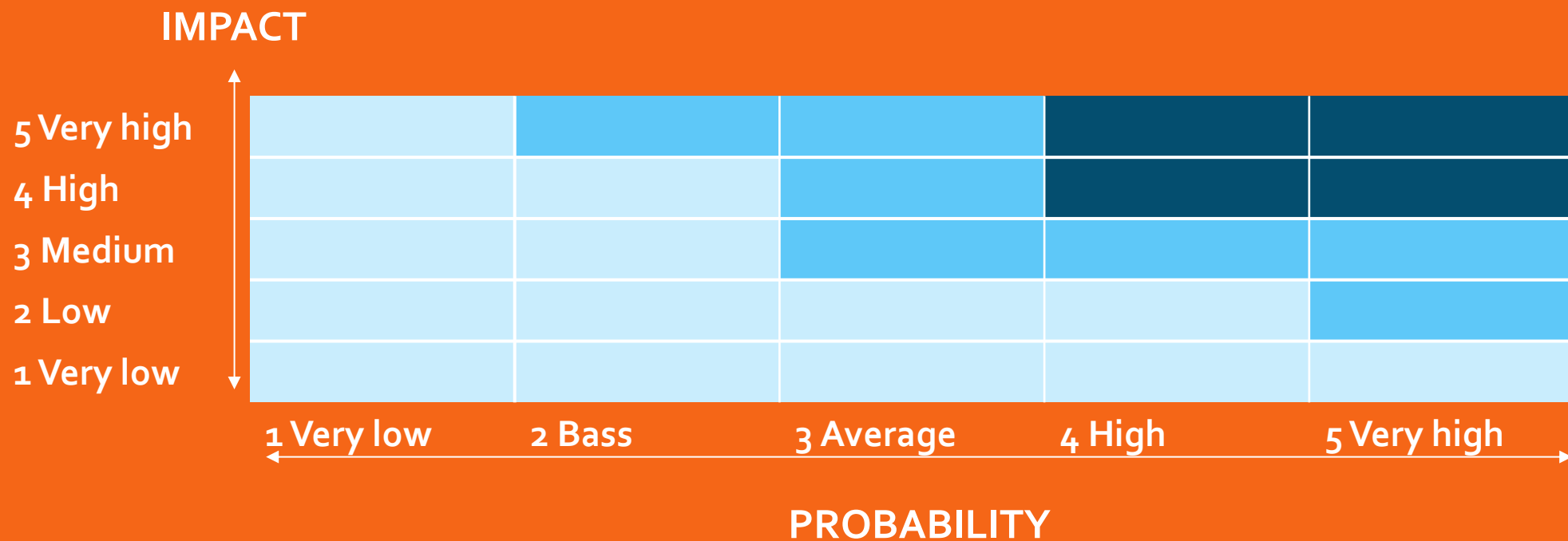
STEP 2 - RISK MATRIX

2.1. DEFINITIONS

PROBABILITY: How likely is it that a risk will materialize? How often can the risk occur? What is the level of exposure?

IMPACT: What would be the impact, the consequences if this risk materialized on staff, programs, etc.?

2.2. RISK MATRIX



	<p>Low risk</p> <ul style="list-style-type: none"> • Standard protocols • Daily security management
	<p>Moderate risk</p> <ul style="list-style-type: none"> • Permanent vigilance • Contingency plan • Specific safety training and meetings
	<p>High risk</p> <ul style="list-style-type: none"> • Immediate response • Emergency plan in working order • Risk reduction/acceptance

STEP 3 - DEVELOPMENT OF AN ACTION PLAN

3.1. RISK REDUCTION OPPORTUNITIES

A safety plan aims to reduce the risk. There are three ways to do this:

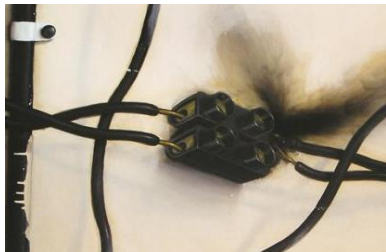
- **Reduced threats**
- **Reduction of vulnerabilities**
- **Capacity building**

➤ **EXERCISE 3:** Find actions to be implemented to achieve each of the building fire reduction opportunities, from the illustrations below:



Reducing threats

Fire prevention in urban areas, ban on campfires in high-risk areas...



Reducing vulnerabilities

Electrical retrofit, reduces the risk of short circuits that can lead to fire.



Increase capacities

Multiplying the number of fire alarms throughout the building (fire extinguishers in all rooms, fire alarms, etc.), makes it easier to fight against the start of a fire



3.2 ACTION PLAN SHEET

- The safety plan must include a sheet for each risk.
- The action plan sheets are in the following format:

Risk X: ... Arrest in connection with a search of the home

Probability: medium to high **Impact:** medium to high

Vulnerabilities: Due process not followed, children at home, sensitive information... ..

Capacities: Be able to predict

Action Plan :

1. Arrange for children to sleep with an aunt when the risk of search is high
2. Do not keep sensitive information at home, delete this information from the computer/phone
3. Knowing my rights in detention, so that I can invoke them peremptorily
4. Inquire about the possibility of installing a surveillance camera to record the event
5. Have a lawyer informed in case I am allowed to see a lawyer

BREAK

Back in 15 minutes

➤ **EXERCISE 6:** Case study in small groups

- Group 1: Cambodia, Indonesia
- Group 2: Ghana, Nigeria
- Group 3: Kenya, Uganda, Palestine

Instructions: In a small group, develop a security plan for your region.

- 1- Appoint a group facilitator
- 2- Appoint a rapporteur to present the work to the whole group
- 3- Apply the two-step methodology to develop a security plan
 - Background analysis
 - Identification of risks, threats, capacities and vulnerabilities (**Risk Formula**)
 - Identify the impact of risks and their probability (**Risk Matrix**)
 - Formulate a security plan to reduce threats, increase capabilities and reduce vulnerabilities to reduce risk.



CHOOSE TWO MAIN RISKS TO WORK WITH.

RESTITUTION

Each reporter has 10 minutes to present the work of his or her group

STEP 4 - DAY-TO-DAY SAFETY MANAGEMENT

4. IMPLEMENTATION AND MONITORING OF THE SECURITY PLAN



Development of the security plan in a participatory manner



Collective ownership by all members



Integration of safety habits into daily activities



Regular risk re-evaluation



Role of the focal points

NEXT STEPS

- Finalize your security plans based on personalized feedback, reminders and new features learned during this session
- Share your security plans with key members of your coalition for feedback (restricted and confidential distribution with "draft" notation)



REMINDER: A security plan is not fixed in time, it must be re-evaluated regularly.

A security plan is a confidential document and should not be shared with everybody.

LUNCH BREAK

SAFETY OF WOMEN HUMAN RIGHTS DEFENDERS (WHRD)

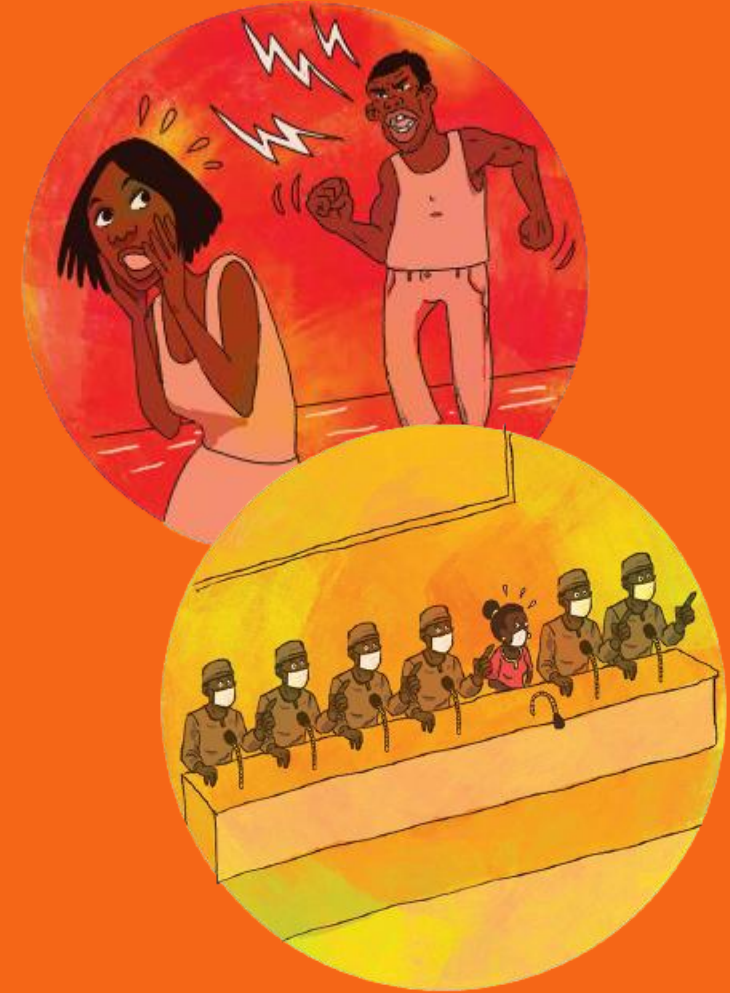
2.1. RISKS TO WHICH THE WHRD ARE EXPOSED

➤ What risks do you think women human rights defenders face specifically?

Participants' responses:

The WHRD must face:

- to violence related to their status as women outside their organization;
- prejudice and discrimination within the HROs, especially those considered as auxiliaries;
- the sidelining of the issue of women's rights and women in decision-making processes;
- hostility towards them because they are contrary to certain cultural, religious and social values regarding the role of women in a country;
- sexual and gender-based violence
- discrediting their professional integrity
- to additional family obligations



2.2. THE SPECIFIC SECURITY NEEDS OF WHRD

WHRD security requires a specific approach:

- Integration/participation of women in decision making alongside men when defining preventive safety measures;
- Take into account women's experiences and perspectives and ensure that they effectively define, verify and evaluate safety rules and procedures;
- Allocate responsibilities for the protection of HRDs within the organisation (e.g. security officers should be familiar with the specific needs of WHRDs, a person trained and competent on the issue of gender-based violence);
- Take into account family concerns and the best interests of the child.



If you identify a particular risk to female members in your coalition, include this risk in your safety plans, including the action plan sheets.



In addition to the security plan, the improvement of the security of the WHRD involves :

- Questioning roles and behaviours, questioning gender stereotypes at work
- Apply positive discrimination to promote change.

2.3. FOCUS: REDUCING/MANAGING THE RISK OF SEXUAL VIOLENCE

➤ REDUCING THE RISK OF SEXUAL VIOLENCE - PREVENTION

- Sexual violence is a form of physical violence; reducing the risk of physical violence also reduces the risk of sexual violence.

➤ MANAGING THE RISK OF SEXUAL VIOLENCE - REACTION

- **Effective medical care** (include in the security budget the purchase of condoms, morning-after pills, triple therapy, etc.)
- **Psychological support**
- **Legal support**



Take gender into account when assisting victims of sexual violence; an assaulted WHRD may prefer the assistance of another woman to that of a man.

BREAK

Back in 15 minutes

3. DIGITAL SECURITY

3.1 RISING CONNECTIVITY

Worldwide	2005	2020
Number of internet subscribers	1 billion	6 billions (74% of the global population)

Source : Statista

3.2. THE DANGERS OF THE INTERNET



DANGERS ON THE INTERNET



PROFILING: automated processing of an individual's personal data to analyze or predict



COMPUTER PIRACY: illegal activities that seek to compromise digital devices (computers, smartphones, tablets, complete networks...)



MONITORING: check the activities of a computer, smartphone, networks, etc. remotely



SHARING: everyone shares everything on the internet, without necessarily asking the opinion of the first person concerned... Image rights, copyright, privacy...



Internet never forgets anything



The published information doesn't belong to you anymore



It has never been so easy to copy and paste



If there is a doubt, there are no doubts



SURFACE WEB

Web

The part indexed by Google and other search engines

4-10%

DEEP WEB

Web

The part not indexed by search engines, but fully accessible legally

90%

DARK WEB

Web

A small part of the Deep Web, accessible only via specialized tools (Tor, I2P...)

1%

3.3 E-REPUTATION

➤ What do you think e-reputation is?

E-REPUTATION: (web-reputation, cyber-reputation, digital reputation) reputation, common opinion (information, opinions, exchanges, comments, rumours...) on the Web of a brand, company, person. It is the perception that Internet users have of it.

➤ What problems do you think are related to e-reputation?

- Rumours
- Misunderstanding of the services and benefits offered
- Reviews

➤ **EXERCISE:** Analyze your e-reputation by typing your name/organization on Google

Share your experience with us!

- Were you surprised by what you found on the Internet about your organization?
- Did you find some things that you thought were deleted?

➤ HOW TO CONTROL YOUR E-REPUTATION?

- Mastering your communication
- Choose your communication vectors
- Protecting your privacy
- Manage the security of accounts, devices and documents
- Use myactivity.google.com



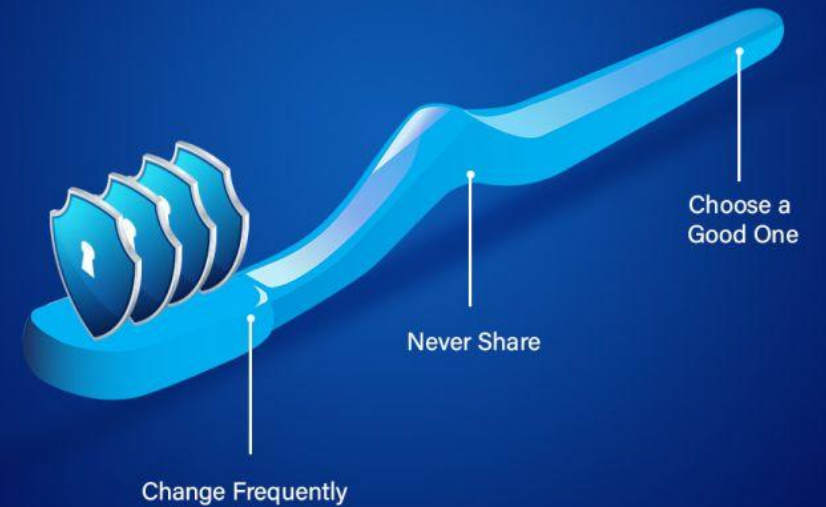
3.4. ACCOUNT SECURITY

➤ IN GENERAL :

- Use privacy-friendly search engines (e.g. Firefox)
- Set complex and different passwords
 - No birthday, no first name
 - Change passwords regularly
- Avoid saving your login information



Passwords are like
Toothbrushes



#cybersecurityawareness


➤ ON SOCIAL NETWORKS

- For couriers
 - Separating the exchange spaces
 - Favour encrypted messaging (Signal, Telegram...)
 - Verify the identity of the interlocutors
 - Activate ephemeral messages
- For the connection
 - Two-factor authentication (Facebook and WhatsApp)
- For visibility
 - Go check the privacy settings of all applications.
(example on Facebook: see where you are connected, what information is public...)
 - Do not post information that is too personal, that could identify your location, etc.



3.5. APPARATUS SAFETY

➤ IN GENERAL :

- To protect against theft:
 - Do not leave devices with sensitive information unattended
 - Put a security code on your devices
- To protect against hacking, profiling and surveillance:
 - Installing an antivirus
 - Regularly delete browsing data (history, cookies, empty caches, etc.).
 - Avoid using public wifi connections
 - Go to secure sites by checking that the URL is `https://` **NOT** `http://` 
 - Avoiding device unlocking by fingerprint



- To protect your information/data:
 - Backup to hidden hard drive/USB stick
 - Lock documents with password
 - If saving online, save to a secure drive (e.g. Nextcloud)
 - Encrypt your emails, use a protected email address (Protonmail for example)

➤ IN CASE OF THEFT OF YOUR DEVICES

How do you react?

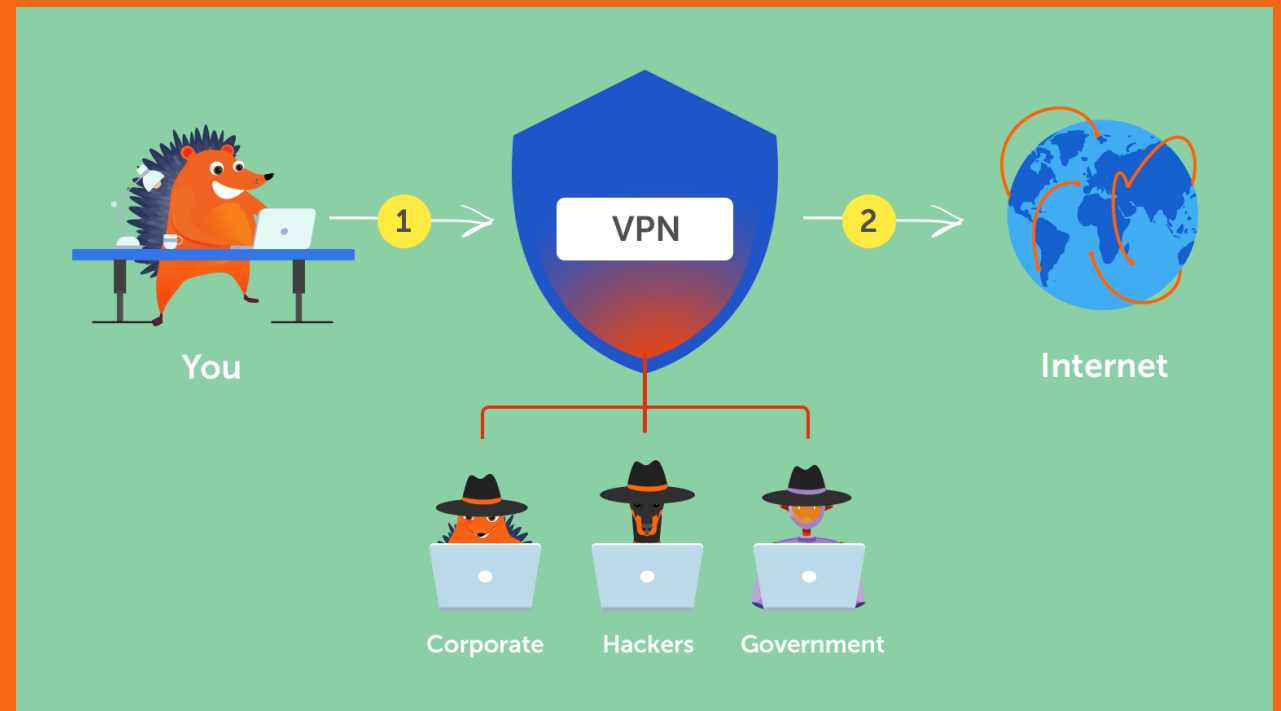
What are you doing to protect the sensitive data on your devices?

- Blocking numbers
- Block the phone (IMEI/chassis number on the packaging or *#06#)
- Disconnect applications (by connecting via another device and then disconnecting from all devices)
- Locate and erase data remotely :
 - Android : android.com/find
 - Apple: https://support.apple.com/kb/PH19300?locale=fr_FR

3.6. VIRTUAL PRIVATE NETWORK (VPN)

What is a VPN?
What is it for?

VPN (Virtual Private Network): a type of computer network that allows the creation of direct links between remote computers via a tunnel through which encrypted information passes.



Source : NameCheap

CLOSING CIRCLE

Any questions?