Information Security for International Researchers

Kieren Lovell
University Information Services
University of Cambridge
To inform users that require information security advice, whilst travelling internationally, in areas that have an increased threat level.
Objectives

1. Why?
2. Advice from Crypto-nerds
3. VPN/Tor
4. Email
5. Mobile Phone / Landline communications
6. Intelligence Profiles & Methods
7. Backup
8. Help from Embassy Staff
9. Overview
10. Questions & Answers
11. References & Contact details
>> Why

1. State Actors
2. Criminal Organisations
1. You are a viable target for both - and they will exchange data.
2. You have money
3. You have status
4. You are international
1. Many people will give you advice
2. Encrypted Mobile Phone / Landline Calls
3. PGP email
1. Do not follow it
2. It will light you up like a Christmas tree
3. The advice here is to keep you off the radar
4. When you are on the radar - it is game over
5. For any advice, please ask us
1. VPN is a great way to have encrypted communications whilst in problematic areas
2. It provides a secure tunnel to another geographical location, until that point, all communications is encrypted
3. Tunnelbear, PureVPN are recommended tools - If you are a mac/PC user, the University of Cambridge provide a VPN service (www.ucs.cam.ac.uk)
4. Do not use this service on an iphone or ipad
1. Tor is a very secure service
2. Works with iphone/android/mac/PC
3. https://torproject.org
4. Slower than VPN, and looks more suspicious if inspecting device
1. Email is as secure as a postcard
2. Email is sent between servers in plain text
3. PGP will only work if everyone you know will use it
4. Protonmail.com will provide you with a free email account that will encrypt communications to anyone. Click the link included in the email, type in a password, and the message will be de-crypted
1. Do not use landline/mobile phone calls for sensitive information
2. Do not use mobile phone/landline encryption voice encryption tools
   *They will hear that the call is scrambled, and assume you are the next James Bond.*
3. VOIP (Skype, SIP etc) - Voice over IP is encrypted. Use over a VPN connection.
1. Do not splash your cash
2. Be weary of communications in public areas
3. Never assume English, or another language, is not understood
4. Stay away from active political gatherings
5. During protests, do not join in, aid, or help.

You will hinder yourself and any cause.
1. If you can, use onedrive  www.uis.cam.ac.uk/initiatives/ees/onedrive
2. Make sure your hard drive (local) is encrypted (MacOS - FileVault, Windows - BitLocker)
3. Do not write your password down. Create a pass phrase.
4. Do not use this password for anything else
5. If you have to use USB to save a backup (Poor internet connection) use an encrypted drive
1. Whilst we are in the EU....... You can use the best embassy in your area, not just the UK. They will treat you like you are their citizen.
2. Look at the FCO website for threat information
3. Contact your local embassy and tell them what you are doing, and get a security brief from themselves
1. Why?
2. Advice from Crypto-nerds
3. VPN/Tor
4. Email
5. Mobile Phone / Landline communications
6. Intelligence Profiles & Methods
7. Backup
8. Help from Embassy Staff
Questions?
References:
1. www.protonmail.com
2. www.tunnelbear.com
3. www.purevpn.com
4. www.torproject.com
5. www.ucs.cam.ac.uk/vpn (Not for ipad/iphone)
6. www.fco.gov.uk

Contact:
Kieren Lovell  -  kieren@lovell.ee - 01223764532
David Modic -  david.modic@cl.cam.ac.uk