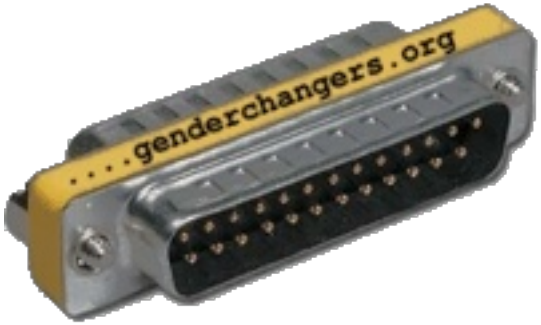

know your hardware

use robust software

physical proximity

keep your passwords on a piece of paper at home and not on your computer

SSL

hand shake

Proxy

cleartext, plaintext and ciphertext

Data Retention

snooping, sniffing and snarfing network traffic, with for example Wireshark

Presumption of Innocence

The burden of proof is thus on the prosecution, which has to convince the court that the accused is guilty beyond a reasonable doubt.

Virtual Private Network (VPN)

SSH, OpenVPN, Hamachi

Note: with a VPN you always need a server at home or elsewhere up and running to manage tunneling your traffic from your remote node.

entropy - a measure of randomness

passwords

"ter qik broun foux jumpies ouver da layz dorg"
"QikBrOUnFoX"

access control

CA - Certificate Authority

Thunderbird & Enigmail are Great!

Key Block = encryption key
Key ID = fingerprint = checksum

PKI - Public Key Infrastructure

PKE

key signing parties

Public-key cryptography, aka asymmetric cryptography

Web of Trust (WoT)

TrueCrypt

cmiua

In general, a PKI enables the parties in a dialogue to establish confidentiality, message integrity and user authentication without having to exchange any secret information in advance, or even any prior contact.

brute force

social engineering

PIA

keylogging

Alice and Bob

phishing

dumpster diving

GCA Security and Privacy workshop 2008-01-07