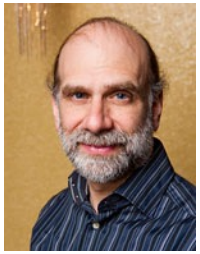
Cybersecurity: Words of Wisdom

by
Bruce Schneier

Who is Bruce Schneier?

- Bruce Schneier is a renowned American cryptographer and computer security professional
- Prolific author of many books including the best-seller *Applied Cryptography*, First Edition, Wiley 1994 (Currently in its 20th Anniversary Edition)
- Author of widely-followed blog "Schneier on Security" (https://www.schneier.com/)



General

- Turn off the computer when you are not using it, especially if you have an "always on" Internet connection

Laptop Security

- Keep your laptop with you at all times when not at home
- Treat it as you would a wallet or purse
- Regularly purge unneeded data files from your laptop

Backups

- Back up regularly
- Back up to disk, tape or CD-ROM
- Store at least one set of backups off-site
- Remember to destroy old backups

Applications

- Limit the number of applications on your machine
- If you don't need it, don't install it
- If you no longer need it, uninstall it

Browsing

- If Internet Explorer still exists on your computer, don't use it
- Instead, use a modern browser such as Modzilla Firefox, Google Chrome, Apple Safari, Microsoft Edge, Opera, Brave
- Limit use of cookies and applets to those few sites that provide services you need
- Set your browser to regularly delete cookies
- Don't assume a Web site is what it claims to be, unless you've typed in the URL yourself
- Make sure the address bar shows the exact address, not a near-miss

Web Sites

- If your browser supports it, install the "HTTPS everywhere" extension
- Secure Sockets Layer (SSL) encryption does not provide any assurance that the vendor is trustworthy or that its database of customer information is secure
- Think before you do business with a Web site
- Limit the financial and personal data you send to Web sites
- Don't give out information unless you see a value to you
- If you don't want to give out personal information, lie

Passwords

- You can't memorize good enough passwords any more, so don't bother
- For high-security Web sites such as banks, create long random passwords and ~~write them down~~ *use a good password manager*
- Guard them as you would your cash
- Never reuse a password for something you care about
- Never type a password you care about, such as for a bank account, into a non-SSL encrypted page
- If your bank makes it possible to do that, complain to them

E-mail

- Turn off HTML e-mail. Don't automatically assume that any e-mail is from the “From” address
- Delete spam without reading it
- Don't open messages with file attachments, unless you know what they contain; immediately delete them
- Don't open cartoons, videos and similar “good for a laugh” files forwarded by your well-meaning friends; immediately delete them
- Never click links in e-mail unless you're sure about the e-mail; copy and paste the link into your browser instead

E-mail

- If you use Microsoft Office make sure macros are disabled
- If you're using Windows, turn off the “hide file extensions for known file types” option; it lets Trojan horses masquerade as other types of files
- Uninstall the Windows Scripting Host if you can get along without it
- If you can't, at least change your file associations, so that script files aren't automatically sent to the Scripting Host if you double-click them

Antivirus and anti-spyware

- Use them — either a combined program or two separate programs
- Download and install the updates, at least weekly and whenever you read about a new virus in the news
- Enable automatically updates feature and set it to “daily”

Firewall

- Spend $50 for a Network Address Translator firewall device
- It's likely to be good enough in default mode
- On your laptop, use personal firewall software
- If you can, hide your IP address (“stealth mode”)
- There's no reason to allow any incoming connections from anybody

Encryption

- Install the *HTTPS everywhere* browser extension that encrypts your communications with many major websites, making your browsing more secure
- Install an e-mail and file encryptor (like PGP)
- Encrypting all your e-mail is unrealistic, but some mail is too sensitive to send in the clear
- Similarly, some files on your hard drive are too sensitive to leave unencrypted
- On a Mac, use *FileVault* and on Windows, use *BitLocker*, *Veracrypt*, *DiskCryptor* or *CipherShed* to encrypt your entire hard drive

Other notable quotes

- “The question to ask when you look at security is not whether this makes us safer, but whether it's worth the trade-off”
- “Security is a process, not a product”
- “People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems”
- “More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk”
- “Data is the pollution problem of the information age, and protecting privacy is the environmental challenge”
- “Amateurs hack systems, professionals hack people”

In chiusura

- 26 Maggio 2022, ore 23.59 — scadenza per consegnare compiti di laboratorio
- 8 Giugno 2022, ore 11.00 (Aula Ercolani E1)— primo appello d’esame (scritto)
- 6 Luglio 2022, ore 11.00 (Aula Ercolani E1)— secondo appello d’esame (scritto)
- Gli appelli d’esame devono essere prenotati tramite AlmaEsami
- Il voto finale si base all'***ultima*** prova sostenuta
- Buone vacanze!