

Conversation with
Fulton T. Armstrong

Who's Spying on YOU?
(and How to Protect Yourself)

Spy Wars

What can we do to protect ourselves?

Broader Solutions??

Update Legislation

U.S. legislation dates back to
1986 (3 years before Web)

Cooperation

Public-private
International
Tech and non-tech firms
Victims

Broader Solutions??

We are signing for Cybersecurity

The digital world is changing everything. It's improving our lives and economies; at the same time, the risk of exposure to cyberattacks is growing dramatically. That's why we are joining forces and have established the Charter of Trust.

Our principles

1. Ownership of cyber and IT security | Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "It is everyone's task."
2. Responsibility throughout the digital supply chain | Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as
 - **Identity and access management:** Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
 - **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes wherever appropriate.
 - **Continuous protection:** Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.
3. Security by default | Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.
4. User-centricity | Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services as well as guidance based on the customer's cybersecurity needs, impacts, and risks.
5. Innovation and co-creation | Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.a. contractual Public Private Partnerships.
6. Education | Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education, and trainings – in order to lead the transformation of skills and job profiles needed for the future.
7. Certification for critical infrastructure and solutions | Companies – and if necessary – governments establish mandatory independent third-party certifications (based on futureproof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions.
8. Transparency and response | Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice which is focusing on critical infrastructure.
9. Regulatory framework | Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of the WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs).
10. Joint initiatives | Drive joint initiatives, including all relevant stakeholders, in order to implement the above principles in the various parts of the digital world without undue delay.

www.charter-of-trust.com



AIRBUS

Allianz

Atos

CISCO

DAIMLER

DELL Technologies

enel

IBM

Munich Security
Conference
Münchner Sicherheitskonferenz

NXP

SGS

SIEMENS

T . .

TOTAL



Charter
of Trust

What YOU can do

12 major steps experts (and I) recommend ...



1. Be smart about passwords

Single most important thing you can do

- Change them.
- Make them unique and long.
- Protect from social engineering.
- **MOST IMPORTANT: E-mail!**

What YOU can do

12 major steps experts
recommend ...



1. Be smart about passwords

Single most important
thing you can do

REPEAT: MOST important thing you can do!!

Get a dedicated password manager

1Password

LastPass

OTHERS:

Dashlane, Enpass, Keeper,
LastPass, LogmeOnce,
RoboForm, and Sticky
Password.



KeePass
Password Safe

Some store on-line, so can “take it anywhere”

BTW ...

Unless you plan to be in
perfect health forever,
don't forget to tell family
where you're hiding your
master password list.



Related to that ...

Do not use Facebook or other social media portal to enter other sites.

goodreads

Discover & read more

Log in to get better recommendations with a free account.



Continue with Facebook



Continue with Amazon

Sign up with email

Already a member? [Sign in](#)

By clicking "Sign up" I agree to the Goodreads [Terms of Service](#) and confirm that I am at least 13 years old. Read our [Privacy Policy](#)



2.



Don't click on links and don't
open attachments!!!!!!!!!!!!

... unless you know
EXACTLY what they
are

CONFIRM WITH
ORIGINATOR
BEFORE CLICKING!!

3.



DO YOUR ROUTINE MAINTENANCE: back up files;
update OS; use good anti-virus, etc.

4.

Use “two-factor authentication”
wherever possible
- Or three-factor, with biometrics

Increasing

New:

 AUTHY

5.

Protect your sensitive data



ENCRYPT: PGP,
VeraCrypt, BitLocker, etc.

6.

Send secure text messages
whenever you can

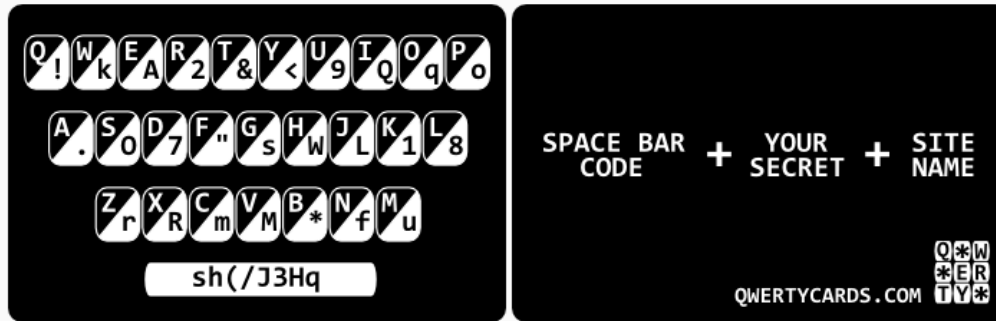
STORE on removable
drive.

WhatsApp, Signal, or other
with end-to-end encryption

Encryption on a card

QWERTYCARD

The simple plastic card that goes in your wallet for easy to remember very strong passwords



Step 1: Type in the code letters shown on the 'spacebar' of the card

Password

Step 2: Enter your own password or secret word

Password

Step 3: Type in the code characters for each letter of the website you are using
Example: www.AMAZON.com use the code characters for each letter of AMAZON

Password



White letters on black are original; black on white are code

HOW TO USE IT >>>>

2. Enter username

3. Enter code on "spacebar"; your secret word; and encoded site name – and ENTER

1. Encode site name – e.g., "Reddit"

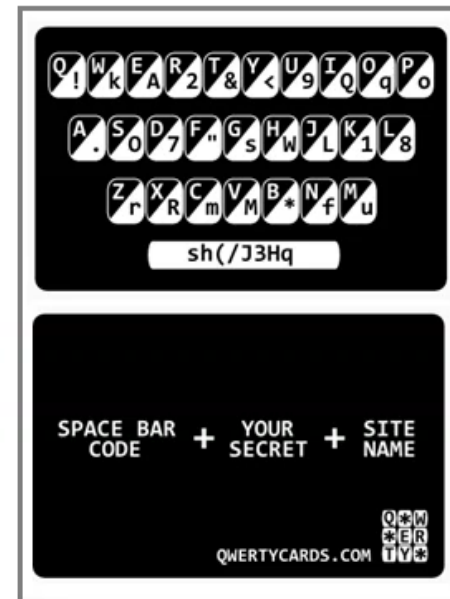


Sign in

SIGN IN

[Forgot username](#) · [Forgot password](#)

New to Reddit? [SIGN UP](#)



R = 2

E = A

D = 7

D = 7

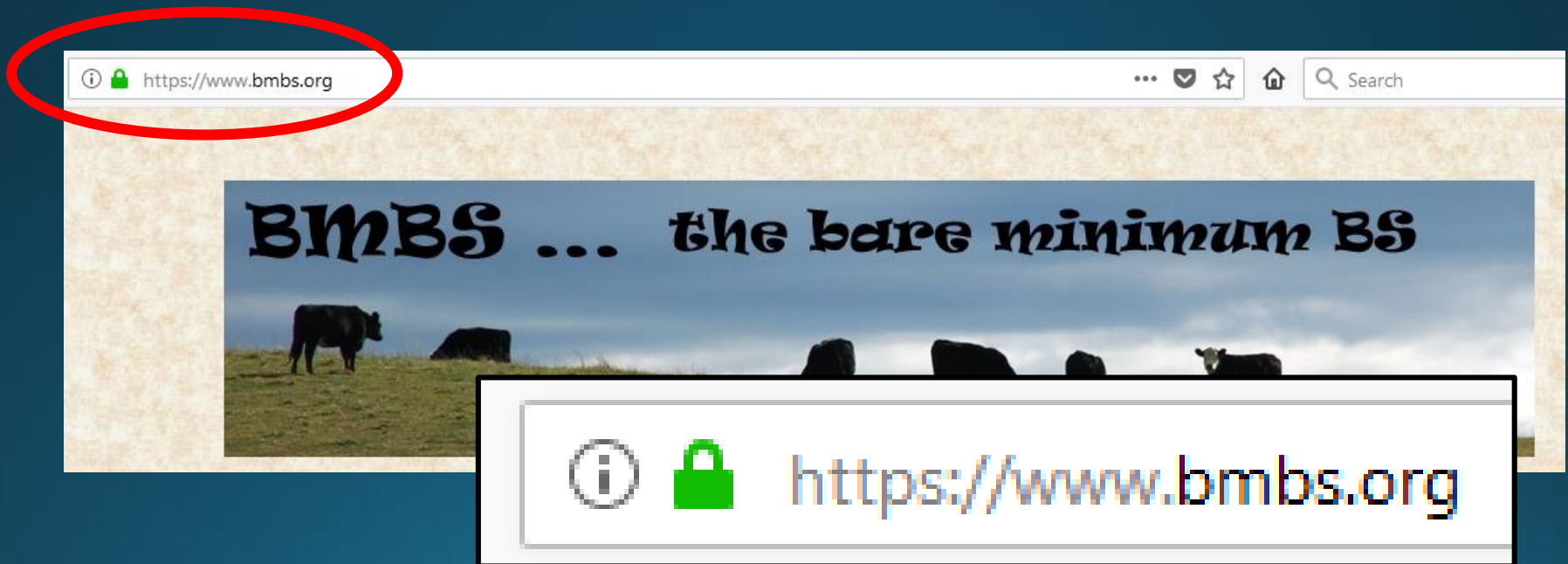
I = Q

T = &

7.



Make sure browser is on HTTPS sites



8.



Use a Virtual Private Network (VPN)

Encryption out of current location

Name	IPVanish VPN	NordVPN	PureVPN	Private Internet Access VPN	KeepSolid VPN Unlimited	TunnelBear VPN	TorGuard VPN	Golden Frog VyprVPN	AnchorFree Hotspot Shield Elite	Hide My Ass VPN
Lowest Price	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT
Editors' Rating	●●●●○	●●●●● EC	●●●●● EC	●●●●● EC	●●●●● EC	●●●●○	●●●●○	●●●●○	●●●●○	●●●●○
Best For	General Users	General Users	Speed Demons	Power Users	Frequent Travelers	First-Time Users	BitTorrent Users	Corporate Users	Novice	Novice
Supported Client Software	Android, ChromeOS, iOS, Linux, macOS, Windows	Android, iOS, macOS, Windows	Android, Chrome, iOS, Linux, macOS, Windows	Android, Chrome, iOS, Linux, macOS, Windows	Android, Chrome, Firefox, iOS, Linux, macOS, Windows	Android, Chrome, iOS, Linux, macOS, Opera, Windows	Android, iOS, Linux, macOS, Windows			
Allows 5+ Simultaneous Connections	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
500+ Servers	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Geographically Diverse Servers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
P2P or BitTorrent	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓

Link to good lists at WWW.BMBS.ORG/spyguy

9.

Turn off your geo-locational data unless you need it



For mobile and browsers

10.

Cover your webcam with tape

11.



Do sensitive searches smartly

Use DuckDuckGo

Bare minimum

Use TOR
("TheOnionRouter") browser

Good but complex
and lightning rod

Go to the library

Use a machine that's not
traceable to you (but no
naughty stuff!)

12.



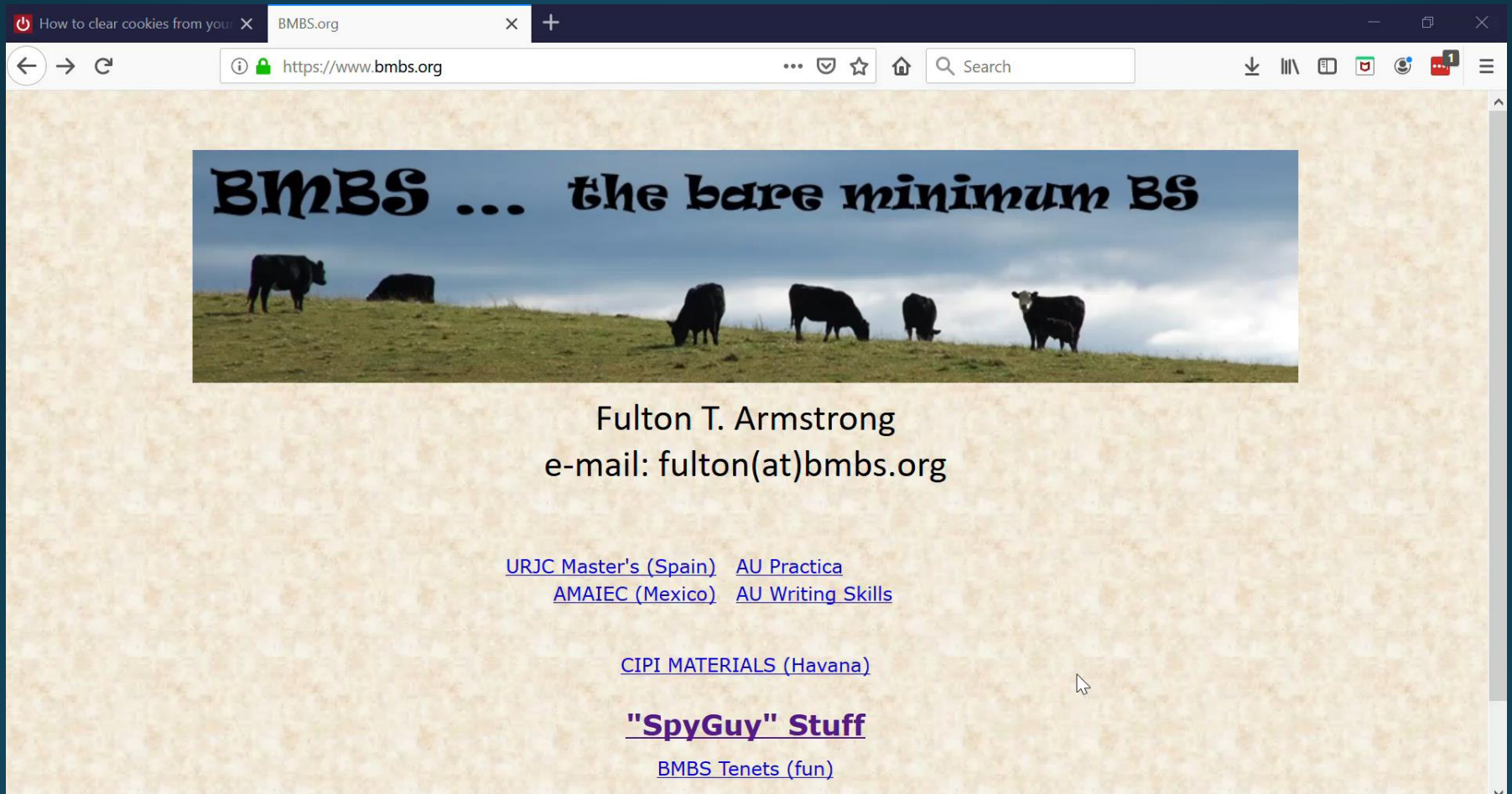
For less-sensitive searches ...

Such as when pricing products ...

Change machines or, better, IP addresses
and DELETE COOKIES between searches.

GOOD PRACTICE: Delete Your Cookies

Example: Firefox (but they're all similar)



How to clear cookies from you x BMBS.org x +

← → ↻ <https://www.bmbs.org> ... 📄 ☆ 🏠 🔍 Search ⬇️ 📄 📄 📄 📄 📄 📄

BMBS ... the bare minimum BS

Fulton T. Armstrong
e-mail: fulton(at)bmbs.org

[URJC Master's \(Spain\)](#) [AU Practica](#)
[AMAIEC \(Mexico\)](#) [AU Writing Skills](#)

[CIPI MATERIALS \(Havana\)](#)

["SpyGuy" Stuff](#)

[BMBS Tenets \(fun\)](#)

“Internet of Things”

Devices upon which we depend

- Electronics
- “Digital Personal Assistant”
- Appliances (including heating and A/C)
- Door locks
- Automobiles

“Alexa”
“Echo”
“Siri”

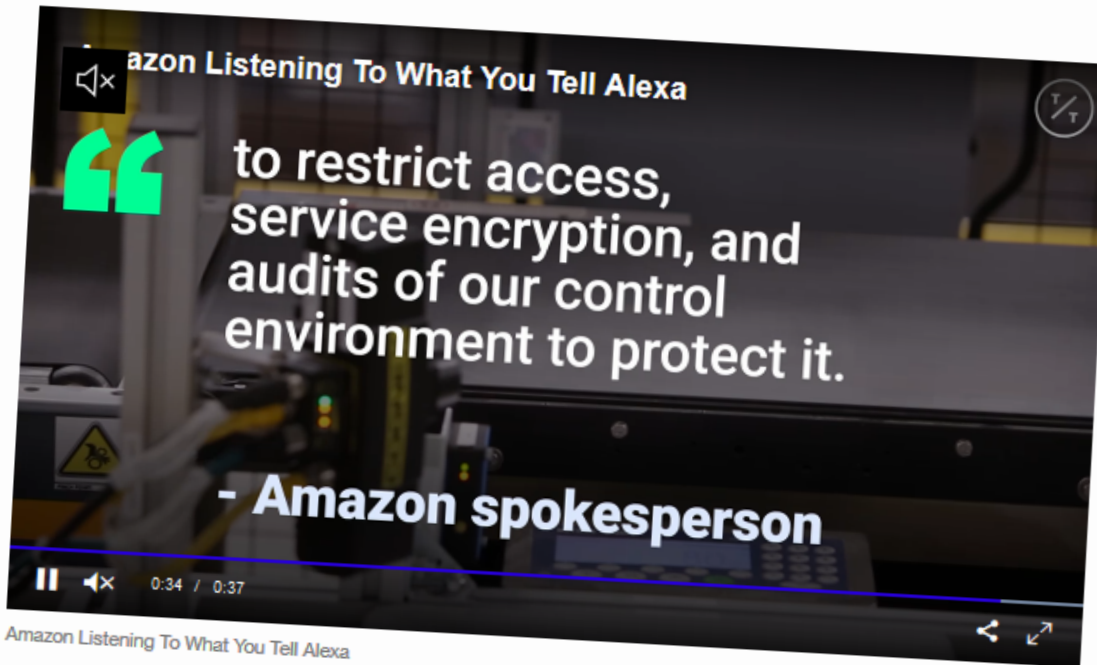
**BE CAREFUL!
USE GOOD PASSWORDS!**

Technology

Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands.

By [Matt Day](#), [Giles Turner](#), and [Natalia Drozdiak](#)
April 10, 2019, 6:34 PM EDT



Amazon Listening To What You Tell Alexa

SHARE THIS ARTICLE

Share

Tweet

Post

Email

Tens of millions of people use smart speakers and their voice software to play games, find music or trawl for trivia. Millions more are reluctant to invite the devices and their powerful microphones into their homes out of concern that someone might be listening.

ALEXA, STOP BEING A PERV Outrage as Amazon's Alexa listens to Brits having sex, rowing, swearing and sharing medical news

EXCLUSIVE

Nick Parker

29 Jul 2019, 22:31 | Updated: 2 Aug 2019, 12:07



Information is power.

This is the new battlefield.

Privacy is no longer an individual right;
it's a national imperative.