
Online
Safety
and
Security

SUBJECTS

Online Threats:

- Malicious Email
- Spam
- Phishing
- Hacked Accounts
- Credit Fraud
- Cyber Harassment

How to protect:

- Home Network
- Mobile Devices
- Passwords
- Accounts
- Online Privacy

Online Threats

Malicious Email:

An email that looks legitimate and urges you to perform an action.

Spam:

Unsolicited, bulk, and unwanted messages by email or digital messages.

Phishing:

Collecting someone's personal intended for malicious. Usually under false pretenses as someone legitimate.

Hacked Account:

When an account is accessed by someone else without permission.

Credit Fraud:

Transactions on a credit card that were not permitted by the card holder.

Cyber Harassment:

Using social media, texting, and/or email to bully or mentally abuse digitally.

Malicious Email & Spam

How did I get it ?

- **Crawling the web for " @" sign.** Spammers and cybercriminals use sophisticated tools to scan the web and harvest email addresses. If you publicly post your email address online, a spammer will find it.

- **Making good guesses… and lots of them.** Cybercriminals use tools to generate common user names and pair them with common domains. These tools are similar to the ones that are used to crack passwords. And they work.

- **Tricking your friends.** Even if you know better than to publicly post your email address on the web, it could still be stored in the email inbox of anyone who's ever emailed you or whom you've ever emailed. Cybercriminals can steal contact lists or use social engineering to trick people into giving them access.

- **Buying lists.** Spammers can purchase lists legally and illegally. When you sign up for a website or a service, make sure you read the privacy policy carefully to find out what the site plans to do with your email address.

Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [redacted] Spam

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>

to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn mo

amazon.com Prime

The Amazon Marketplace

------SHOPPER/MEMBER:4726
------DATE-OF-NOTICE: 12/22/2015

Hello Shopper:[redacted]@gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

Please visit-here now to get your reward

***DON'T WAIT! The Link Above Expires on 12/28!

Ignore Junk Delete | Reply Reply All Forward Meeting More | Awards Team Email Reply & Delete To Manager Done Create New | Move Rules OneNote Actions | Mark Unread Categorize Follow Up | Translate Find Relate Select

Delete | Respond | Quick Steps | Move | Tags | Editing

Wed 11/11/2015 06:07

Department of National Defence Canada <[redacted]>

SECURITY TIPS FOR [redacted]

To [redacted]

Message SECURITYTIPS2015.zip (114 KB) Department of National Defence.pdf (324 KB)

Department of=National Defence
Counter Terrorist uni=

TO: [redacted]

Sir,

We got a terror alert regarding your business area.

Be advised to follow the protective measures (SECURITY TIPS) as attached to keep yourself, your compa=y and your family secured

Best regards,

[redacted]

https://www.pcworld.com/article/3072435/data-center-cloud/5-ways-to-stop-spam-from-invading-your-email.html

https://knowtechie.com/prevent-phishing-attack-infographic/

Hacked Accounts & Credit Fraud

Know the Signs

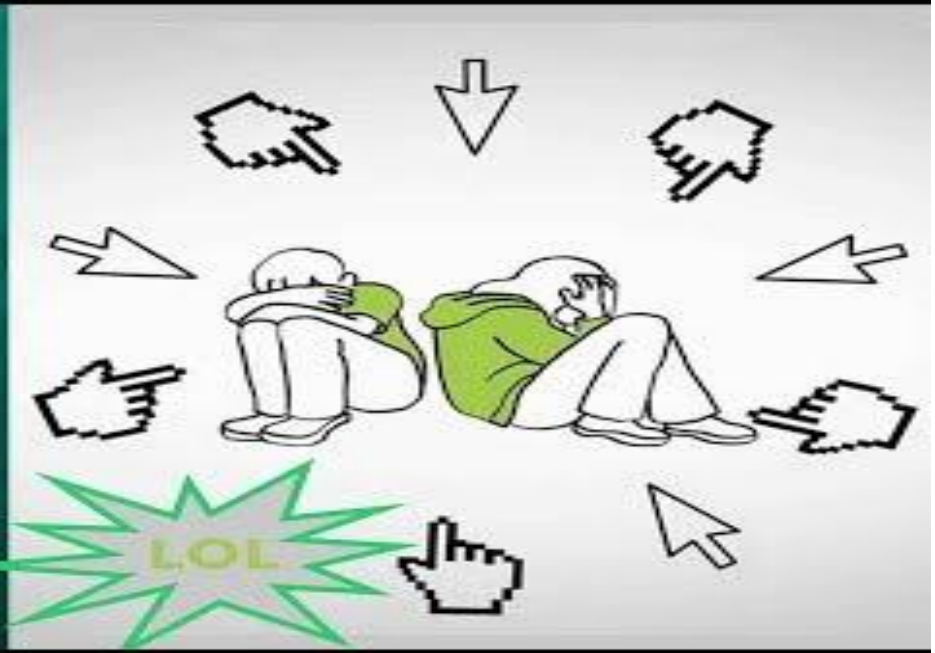
- Mysterious activity
- Alert email or text that password or pin number have changed.
- Email alert from web host / business

What to do:

1. Contact the ***"REAL"*** source directly
2. Gain control of your assets
3. Reinforce security and authentication

Cyber-bullying Facts

Top 10 Forms of Cyber Bullying



...you breaching copyright, but you are also making your devices vulnerable to viruses.

How to always stay a step ahead of the cyber thieves

FROM PREVIOUS PAGE

than a laptop and phone, to create their own wifi network and lure unsuspecting users to join it. Once you do so, the criminal can then steal your personal information.

This means you should only use wifi networks that you recognise and trust. If in doubt, ask the owner of the cafe, restaurant or shop you are in. And if you're unsure, don't use wifi to connect to the internet — instead, use your device's mobile connection.

WHAT'S SAFE TO DOWNLOAD?

YOU may be aware that thieves try to infect computers with viruses. Often, these are spread via email, and are installed on computers when an unwary recipient clicks on an attachment. Do not download anything, or click on anything — whether in an email or a webpage — that looks suspicious.

Tablet and smartphone users should also be wary of apps they download. Although they should never have viruses, sometimes they have connections to other apps on your device, such as Twitter and Facebook, and unscrupulous software developers can use these connections to access your details.

DO I NEED VIRUS SOFTWARE?

THIS is a must — and ignore people who say you don't need such software on Apple products, or on tablets — you do! In order to protect your data and your computer, it is worth installing antivirus software — such as Avira, which is free and available from the Play Store and Apple App Store — that runs constantly and checks that no hackers are trying to gain access to your device.

can crack your password on, say, Amazon, they will then try your online bank account using the same password.

HOW TO BANK ONLINE SAFELY

THERE'S no doubt that online ...

the conmen by remembering these steps:

1 CHECK that you have an "https" connection when you login. Before you log in to your account, look to see if the bank's web address in the browser bar starts with 'http' or 'https'. That extra 's' stands for 'secure', and this is what you need to see. Sites that just begin with 'http' are not secure, and you shouldn't enter any private information into them.

2 LOOK for the padlock! All secure sites feature a padlock icon in the browser bar. If you click on the padlock, a window will pop up featuring a security certificate, which will show that the website's owner has been verified. If you do not see the padlock, under no circumstances log in.

3 CHECK the web address. This may seem obvious, but make sure you have entered your bank's web address correctly. Many criminals try to register site names that look very similar to the correct address, or sites that are spelled like real addresses, but with common typing errors.

Keep your details safe

AGAIN, this may seem like common sense, but do not share your log-in details with anybod... Neither should you write the... down — especially not on... sticker attached to the screen... your laptop!

Check your bank account regularly

IDEALLY, you should log... your bank account every d... have a look through all... recent transactions.

In addition, if your ban... it, subscribe to a text... service that will sen... weekly or daily balanc... mobile phone.

Tech tip

Make the most of your broadband by buying a new, superfast router. If yours is over two years old, consider replacing it

HOW TO SHO... ONLINE SA...

SHOPPING online... growing business... comes with a risk... know if your cred... are secure? Follo... safe shopping:

Do I Need Antivirus?

AntiVirus and AntiMalware Software

Norton from symantec

Malwarebytes

avast

C Cleaner

AVG

SUPER AntiSpyware

Bitdefender

https://www.top10bestantivirus.com/best-free-antivirus?gclid=EAIaIQobChMI083t95Tm3QIVVrXACh35kgAYEAAYAyAAEgKOc_D_BwE

PASSWORDS ARE LIKE UNDERPANTS

Change them often, keep them private and never share them with anyone.

REPORT

Password Manager Apps

Dashlane: #1 Password Manager

F-Secure KEY Password manager

1Password - Password Manager

Password Manager

My Passwords

Keeper®: Free Password Manager

Avast Passwords

Hide Pictures Keep Safe Vault

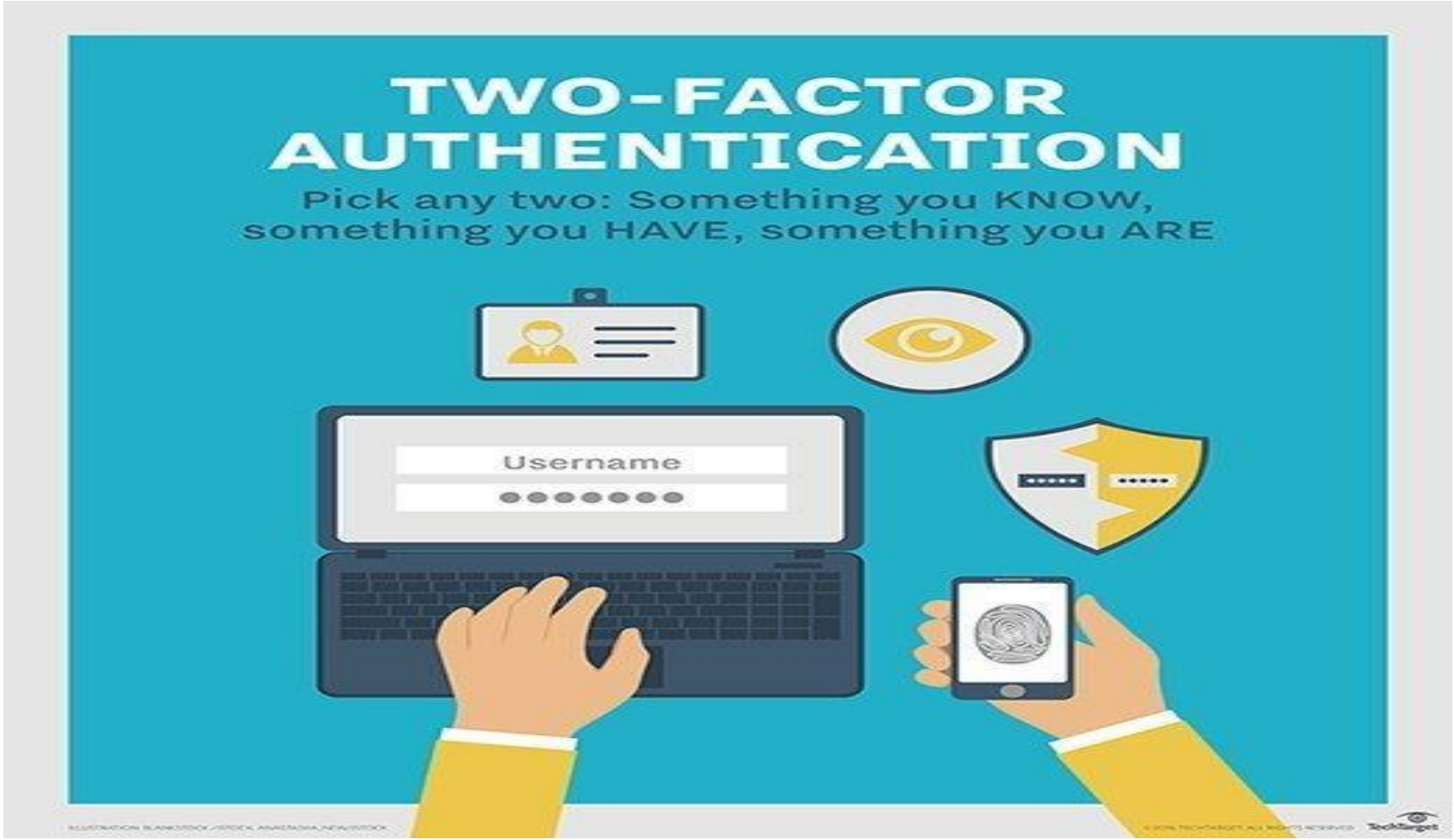
LastPass Password Manager

https://thehackernews.com/2017/02/password-manager-apps.html

Main advantages of using password manager:

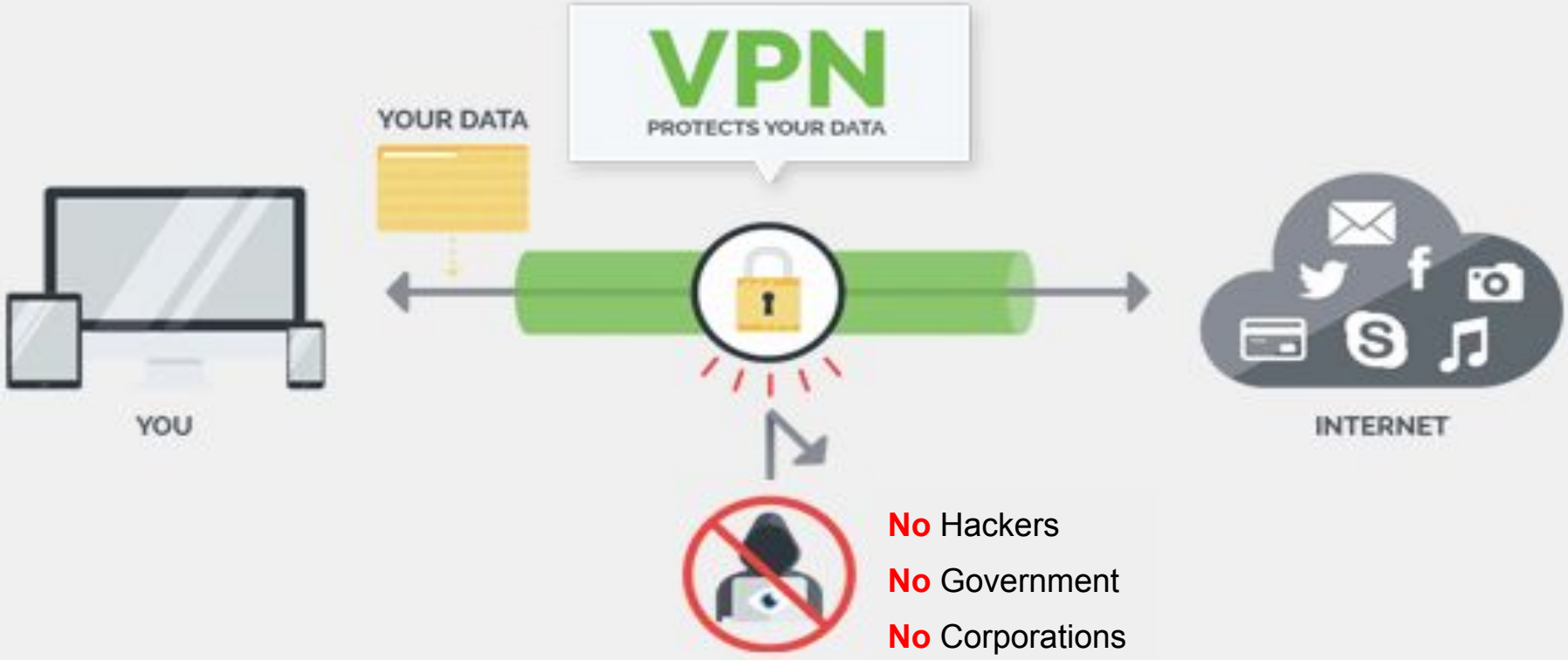
- Create reliable and strong passwords in seconds
- Autofill your login credentials on websites with just a single password
- Two-step authentication for added security

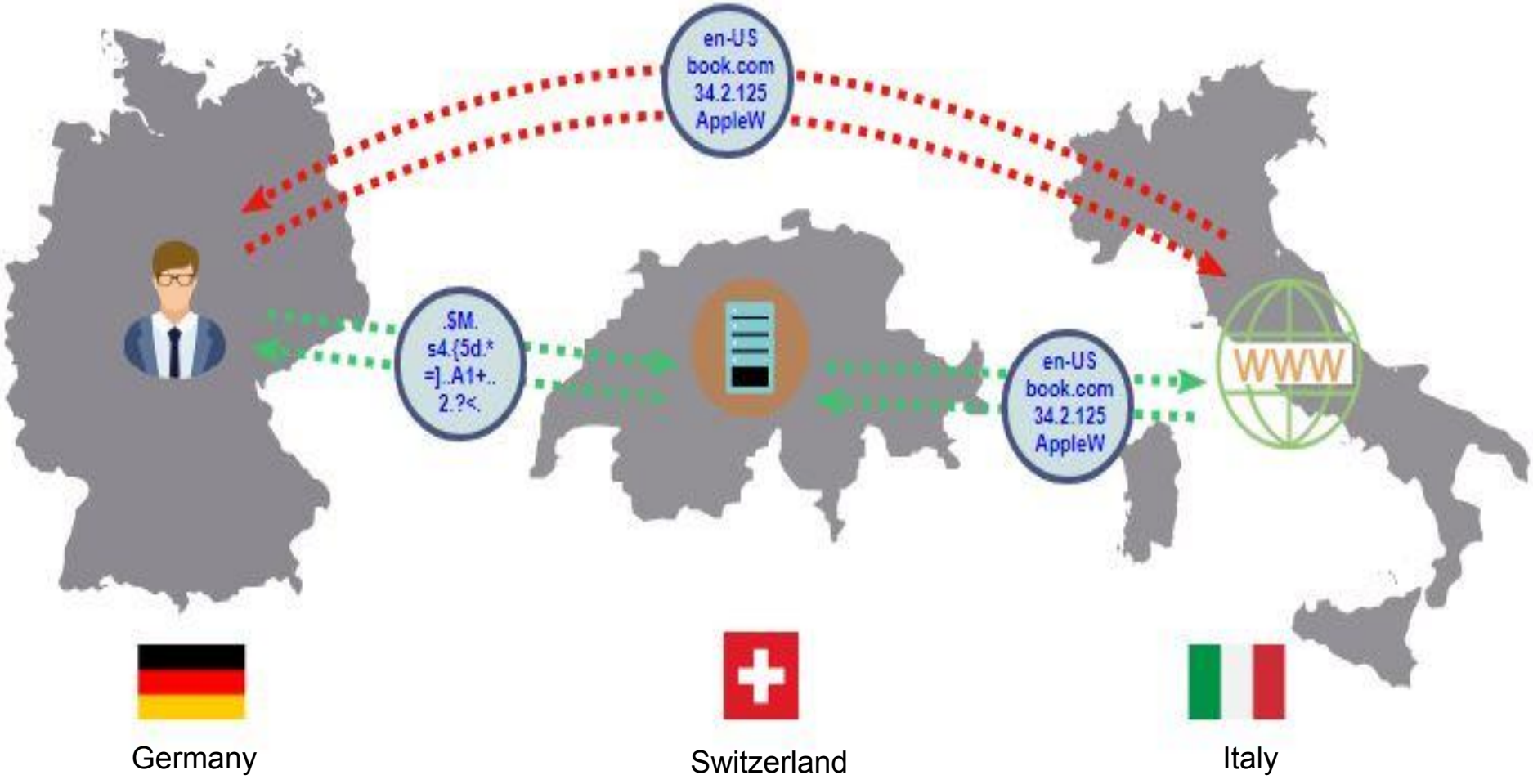
https://techspective.net/2018/04/23/what-is-a-password-manager-and-why-do-you-need-it/



https://www.g2crowd.com/categories/multi-factor-authentication


YouTube


VPN
PROTECTS YOUR DATA
YOUR DATA
YOU
INTERNET
No Hackers
No Government
No Corporations


en-US
book.com
34.2.125
AppleW
.SM.
s4.{5d.*
=]..A1+..
2.?<.
en-US
book.com
34.2.125
AppleW
WWW
Germany
Switzerland
Italy


COOKIE


HELLO

Summary

1. Use an Anti-Virus & Anti-Malware on your devices.
2. Look into using a VPN for mobile and home PC.
3. Be careful on what you *CLICK* online and in email.
4. Always question your sources on the internet.
5. Start using Two Way Factor Authentication **TODAY**.
6. When in doubt do some research and a reliable source.

Let’s talk about some bad & good stuff

Ransomware: Hacker Locks Guests out of Rooms

http://www.slate.com/articles/technology/future_tense/2017/02/the_ransomware_attack_that_locked_hotel_guests_out_of_their_rooms.html

Opening up Email ***USED*** to be ***MEGA*** Dangerous

https://www.howtogeek.com/135546/htg-explains-why-you-cant-get-infected-just-by-opening-an-email-and-when-you-can/

Facebook Hacks 50 Million Users

https://www.cnbc.com/2018/10/03/facebook-hack-faq.html

No More Weak Passwords in California

https://www.wired.com/story/security-news-this-week-good-news-california-bans-bad-default-passwords/

China uses hardware to Hack Apple and Amazon

https://finance.yahoo.com/news/apple-amazon-deny-bloomberg-report-110439954.html

AT&T Fails to Doing its Own Safety Protocol

https://www.theregister.co.uk/2017/07/10/att_falls_for_hacker_tricks/