

DIGITAL SECURITY 101

By Ronalyn V. Olea | Bulatlat, NUJP

WHAT IS DIGITAL SECURITY?

The protection of one's digital or electronic identity

Digital footprints:

Browser cookies

Persistent logins on mobile device and web eg. Facebook, Google

Logins

IP Address + connections

Metadata in photos, documents, social media posts

Mobile tower access (~500m), calls

WiFi connections (even if not connected)

DATA STORED IN YOUR DEVICES

Lost or stolen mobile devices =
unauthorized access, data theft

List down all the important data in your
mobile phones and/or laptops





I have been seeing posts from people with [#BDO](#) accounts saying someone else purchased online using their debit cards (without their knowledge).

Today I checked my account and there, someone got to use my account details to purchase an item worth 1,800+ from an online shop based in the US. So I immediately went to my branch and had my card blocked. BDO assured me they will investigate on this unauthorized transaction.

Has anyone here experienced a similar case?

Fellow BDO customers, please check your accounts always.

PS You can always check your card/account's transactions through your mobile app.



13 Comments 10 Shares

**WHY SHOULD YOU
BE MINDFUL OF
YOUR DIGITAL
SECURITY?**

Public school teacher in debt because of identity theft

Published February 26, 2016 10:48pm

A public school teacher may be a victim of identity theft as he owes three banks P800,000 for loans he did not apply for, according to a report by John Consulta on GMA-7's "24 Oras" on Friday.

Mark Joseph Lontok said he received notifications from three banks saying that he borrowed a total of P800,000 in salary loans. He denied applying for the loans.

However, Lontok remembered posting a photo of his Professional Regulation Commission (PRC) ID online.

"Iyong time na nakapasa ako sa LET (Licensure Examination for Teachers), nag-post po agad ako. Tsaka pagpasok ko po sa public (school), pagbigay ng papel ko, pinost din po sa FB (Facebook) sa

**WHY SHOULD YOU
BE MINDFUL OF
YOUR DIGITAL
SECURITY?**

CYBERCRIME | HACKING

COMELEC breach data released online, fully searchable

Posted: April 21, 2016 by [Christopher Boyd](#)

On March 27, the [COMELEC](#) (Philippines' Commission on Elections) website was defaced and data on up to 55 million registered voters in the Philippines was [compromised](#).

At the time, a COMELEC spokesman stated that "There is no sensitive information there".

Presumably frustrated by the response, one hacker (or group of hackers) have decided to deposit all of that voter data onto a searchable website and let people make up their own minds as to what constitutes "sensitive information". From the text on the site, it appears that the people behind this aren't related to those who performed the initial breach.

**WHY SHOULD YOU
BE MINDFUL OF
YOUR DIGITAL
SECURITY?**

TECHSPOT


LOGIN

TRENDINGFEATURESREVIEWSTHE BESTDOWNLOADSVIDEOPRODUCT FINDERFORUMS


Government requests for Facebook user data up 21% during first half of year

The company just published its transparency report

By Rob Thubron December 19, 2017, 1:28 PM | 10 comments



MOST READ



31 comments

AMD FSR 2.0 vs. DLSS: 8 Generations of GeForce and Radeon GPUs Benchmarked

20 minutes ago

'Very powerful story': Top Biden aide concedes...

Edward Snowden: Facebook is a surveillance company rebranded as 'social media'

by Daniel Chaitin | March 17, 2018 09:28 PM

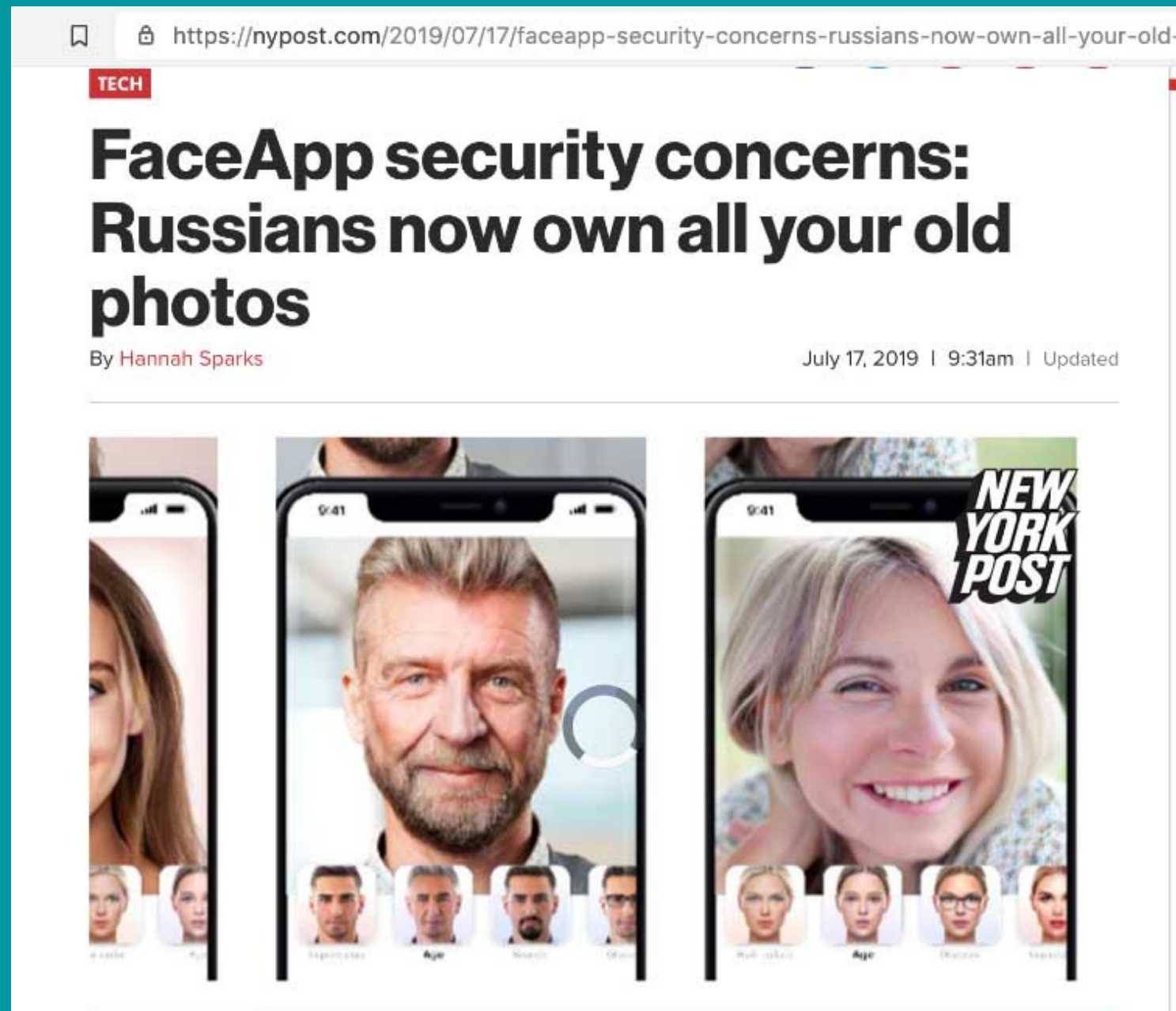


WHY SHOULD YOU
BE MINDFUL OF
YOUR DIGITAL
SECURITY?



The data, a portion of which was viewed by The New York Times, included details on users' identities, friend networks and "likes." The idea was to map personality traits based on what people had liked on Facebook, and then use that information to target audiences with digital ads.

**WHY SHOULD YOU
BE MINDFUL OF
YOUR DIGITAL
SECURITY?**



FaceApp, which you grant permission to access your photo gallery, also includes in their Terms and Conditions that they have the right to modify, reproduce and publish any of the images you process through its AI.

**WHY SHOULD YOU
BE MINDFUL OF
YOUR DIGITAL
SECURITY?**



WHY SHOULD YOU
BE MINDFUL OF
YOUR DIGITAL
SECURITY?

A hacker attacks someone's privacy every 39 seconds.
On average, it is equivalent to 2,244 times a day

BASIC SECURITY

Setup a Screen Lock

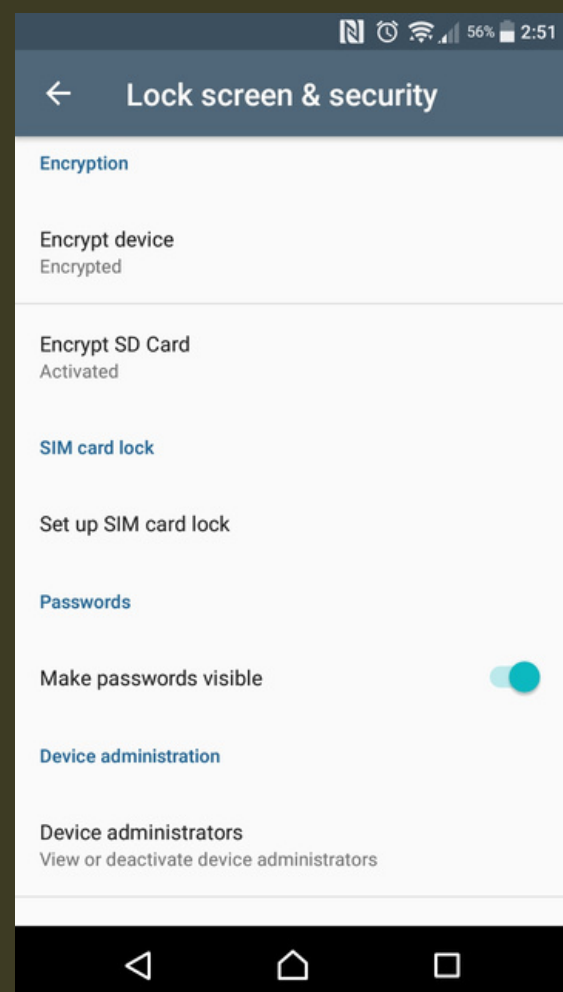
Settings-> Personal -> Security -> Screen Lock

Set the security lock timer, which will automatically lock your phone after a specified time.

Enable Lock SIM card

Settings -> Personal -> Security -> Set up SIM card lock

BASIC SECURITY



Encrypt device and SD card

Android: go to Settings, Lock Screen & Security

iPhone: go to General Settings and Set Passcode

GENERAL PRECAUTIONS

- Keep devices with you at all times. Never leave your phones or tablets out in public.
- Use a security code. Add a Personal Identification Number
- Monitor for tampering. Mark your device with something unique and not immediately noticeable to help you identify it
- Use tamper-proof security tape at the edge of devices that open easily (especially when asked to leave your cellphones)

PROTECT YOUR DELIVERIES!!!

BAKEREX the bakery exchange, inc. **TAMPER-PROOF SECURITY TAPE**



BEST FOR:
SENSITIVE DOCUMENTS
FOOD DELIVERIES
HIGH VALUE ITEMS

AVAILABLE IN 2 SIZES & COLORS
BROWN TAPE 30mm x 10 meters
YELLOW TAPE 50mm x 10 meters

EMAIL:
inquiry@bakerex.com

Grab/Lalamove etc. for Account of Buyer

GENERAL PRECAUTIONS

- Keep your IMEI (International Mobile Equipment Identity) number separate from your phone.

- helps you trace and prove ownership if your phone is stolen. Reporting it to service providers will block the device.

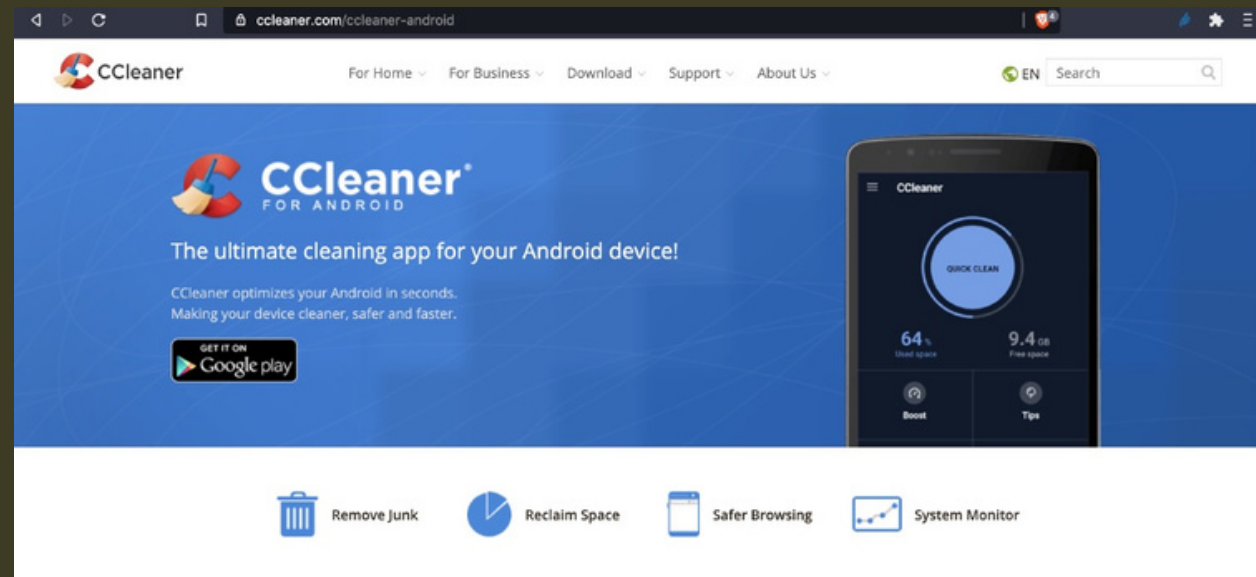
To find your IMEI:

Key *#06# into most phones

Look behind the battery

Check the phone settings

GENERAL PRECAUTIONS



- Install anti-virus. Some phones have their own AV. (Avast, BitDefender, Malwarebytes, Avira etc.)
<https://fossbytes.com/best-android-antivirus-apps/>
- Install CCleaner for Android to delete files and clean digital footprints.

BASIC SECURITY

- Keep your software updated.

Settings -> About phone -> Updates -> Check for updates

- Turn off Wifi and Bluetooth by default. Ensure that Tethering and Portable Hotspots are switched off when not in use.

Settings -> Wireless and Networks-> More -> Tethering and mobile hotspot

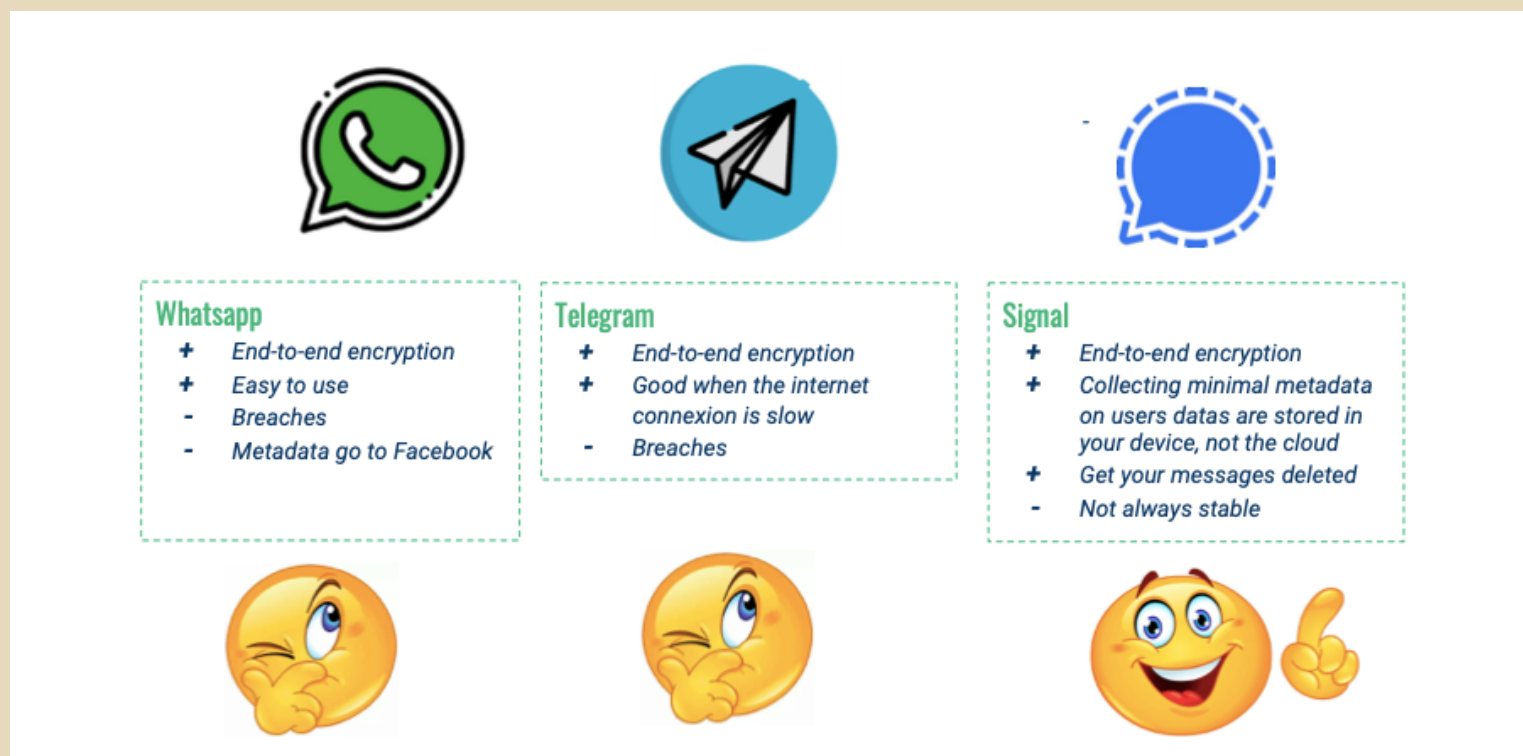
- Backup the contents of your phone regularly. Use encrypted devices (SIM, OTG, hard drive)

MOBILE APPS

Mobile apps can pose serious threats. Malicious apps can spy on your device, collect information about your activities, read your messages, or copy and send information from your phone to a remote server.

- Download apps from official app stores.
- Limit the number of apps you install to the bare minimum and install apps you need only.
- Review your existing apps permissions and disable all permissions to your location, camera, contacts, messages and mic unless needed for the apps to work. Choose to disable these permissions and enable only when using the app.
- When installing a new app, make sure it is from a legitimate developer, examine the app permissions. Check the app history and when it was last updated.

SECURE COMMUNICATIONS

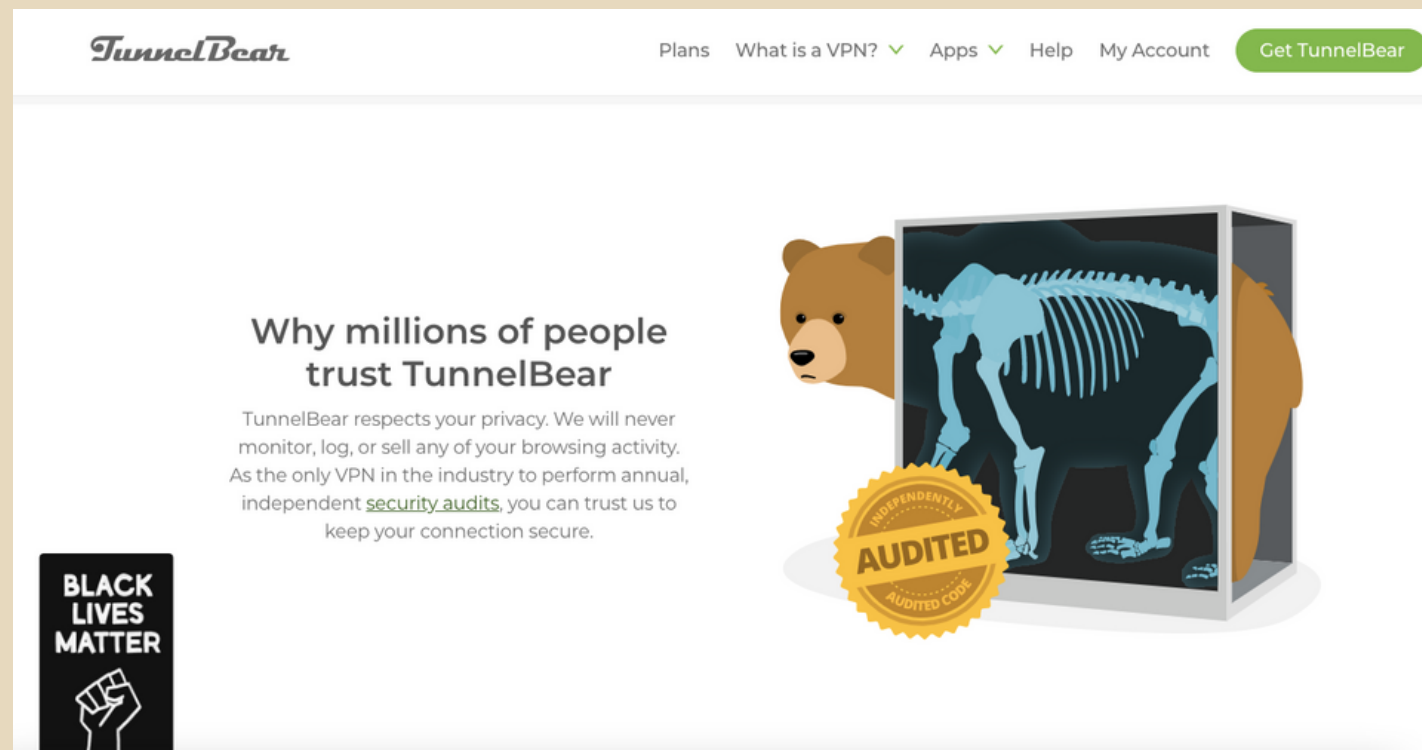


- Do not autosave your username and passwords
- Use Signal for encrypted communications

<https://www.securemessagingapps.com/>

- Use the internet securely

SECURE COMMUNICATIONS



- Use VPN (Tunnelbear, Psiphon, ExpressVPN, ProtonVPN)
- Do not connect to a public Wifi

SMART PHONES AS TRACKERS

Any phone can be tracked via mobile phone towers via triangulation and any data/SMS/calls made

Anti-Terror Act allows surveillance of computer data of 'suspects'

Prepaid or post-paid?

Do you need to carry your phone?

LAPTOP



- Set a non-admin account & use for daily use
- Set a strong password
- Install and update AV (Avast, Malwarebytes)
- Never leave your computer unlocked
- Keep OS and software updated
- Encrypt part of your hardware
- If you connect to a public wifi, use VPN

PASSWORDS AND SOCIAL MEDIA

HOW SECURE IS YOUR PASSWORD?

<https://www.security.org/how-secure-is-my-password/>



PASSPHRASES

Choose an obscure statement or quotation that will not be easily linked to you by others.

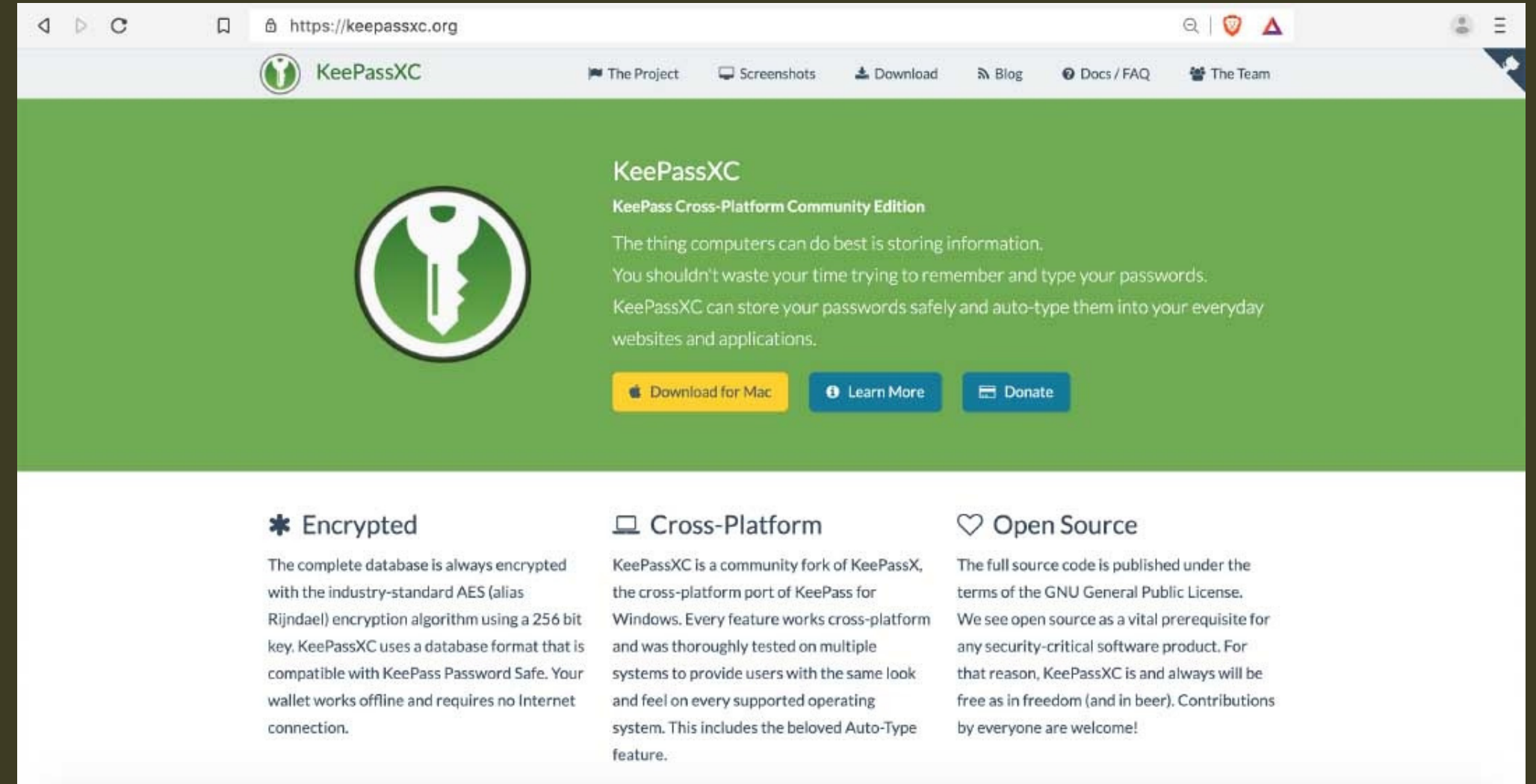
You can use the whole phrase or abbreviate it to create a series of letters and numbers.

For example: “Why is it always so hot outside?”
→ WiiA50HO? “That toy tiger I had as a kid was the best!” → TtT1hadAak1Dwa5th3B!

Do not use the same password for multiple accounts.

Change your passwords regularly.

PASSWORD MANAGER



Store your passwords in a password manager.
KeePassXC or Bitwarden
<https://ssd.eff.org/module/how-use-keepassxc>

Be sure to have a backup stored in an encrypted device.

QUESTIONS WHEN USING SOCIAL MEDIA

- How can I protect my identity, my privacy and my contacts?
- What information do I want to keep private?
- Who do I want to keep it private from?

5 DANGERS OF FACEBOOK

Facebook admits to wrongly sharing user data with third party apps yet again

By [Jasmine Gearie](#) July 02, 2020

Facebook tries to save face, again



(Image credit: Shutterstock)

1. Your information is being shared with third parties.

Facebook's mission is to get you to share as much information as it can so it can share it with advertisers.

Every time you take popular quizzes, you authorize an application to be downloaded to your profile that gives information to third parties about you that you have never signed off on.

5 DANGERS OF FACEBOOK

1. Your information is being shared with third parties.

The social media giant estimates the error saw around 5,000 third-party app developers continue to receive information about users who had previously used Facebook to sign into their apps, even if users hadn't used the app in the past 90 days.

(<https://www.techradar.com/news/facebook-admits-to-sharing-users-personal-data-with-third-party-apps-yet-again>)

5 DANGERS OF FACEBOOK

2. Privacy settings revert to a less safe default mode after each redesign.

Facebook does not [necessarily] notify you of the changes, and your privacy settings are set back to a public default.

5 DANGERS OF FACEBOOK

Facebook: Malware that took over accounts and placed scammy ads a growing risk

The company says it stopped a malware campaign in its tracks, but warned that hackers will keep targeting users of Facebook and other social media platforms.



Laura Hautala · Oct 1, 2020 11:01 a.m. PT



▶ LISTEN - 02:37



3. Facebook ads may contain malware.

Facebook has not been able to screen all of its ads. It hasn't done a great job of vetting which ads are safe and which are not.

5 DANGERS OF FACEBOOK

4. Your real friends unknowingly make you vulnerable

Your security is only as good as your friend's security. If someone in your network of friends has a weak password, and his or her profile is hacked, he or she can now send you malware, for example.

There is a common scam in which someone hacks your profile and sends messages to your friends asking for money - claiming to be you.

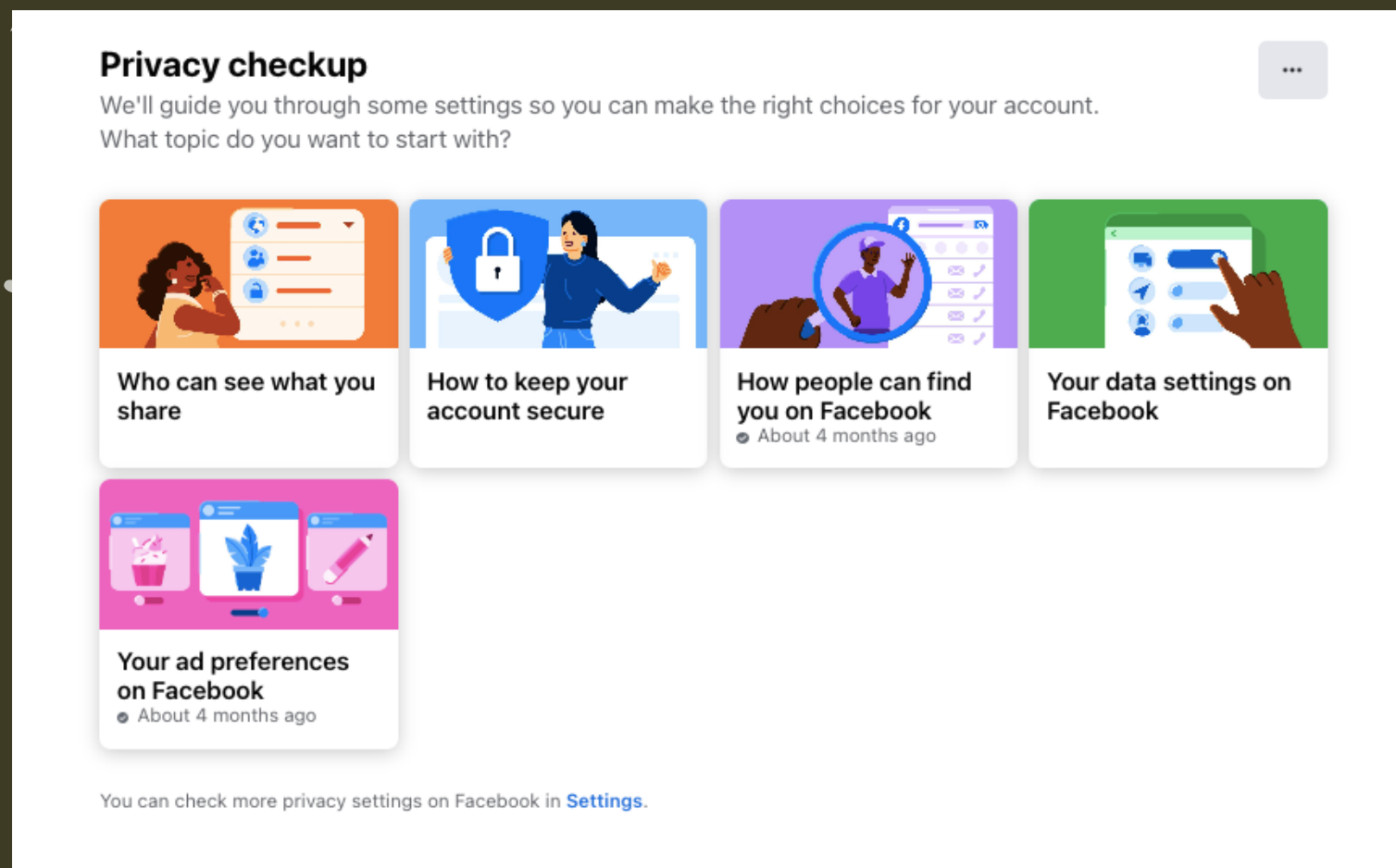
5 DANGERS OF FACEBOOK

5. Scammers are creating fake profiles.

40 percent of all FB profiles are fake.

Source: <https://www.cnet.com/news/five-hidden-dangers-of-facebook-q-a/>

SECURITY CHECKS



Facebook

<https://www.facebook.com/help/443357099140264>

Twitter

<https://help.twitter.com/en/safety-and-security#ads-and-data-privacy>

Instagram

<https://mashtips.com/instagram-privacy-settings/>

GENERAL RULES

- Use strong passwords. Change it frequently. Use password manager (Bitwarden or KeePassXC)
- Activate 2FA on all your accounts
- Use separate social media accounts for professional, personal use. Consider using pseudonyms for different activities (buying online, connecting with former classmates, etc.)

GENERAL RULES

- Never log in to 3rd party apps using your social media accounts.
- Set limits and discuss with friends.
- Never access social media from device or network that you don't trust, or a public computer that may store password or browsing history

GENERAL RULES

- Never log in to 3rd party apps using your social media accounts.
- Set limits and discuss with friends.
- Never access social media from device or network that you don't trust, or a public computer that may store password or browsing history

2-FACTOR AUTHENTICATION

The vulnerability of passwords is the main reason for requiring and using 2FA.

90% of passwords can be cracked in less than six hours

Sophisticated cyber attackers have the power to test billions of passwords every second.

2-FACTOR AUTHENTICATION

Two-factor authentication (2FA) is a second layer of security in addition to a password that a user must provide before being granted access to an account or system.

This drastically reduces the chances of fraud, data loss, or identity theft.



Download Authy app on your mobile phone.

Enable 2FA on your Facebook account or Gmail account.

Video tutorial:

<https://www.youtube.com/watch?v=7gsBG6Nt21k>

Authy for Google and Gmail accounts

<https://authy.com/guides/googleandgmail/>

ONLINE PRIVACY AND SECURITY

CHOOSING THE RIGHT BROWSER

Go to <https://coveryourtracks.eff.org/>
to check your browser





Google Chrome

The company collects a lot of personal information about you.



If you want to maximize your privacy, install these add-ons:

Privacy Badger

Cookie Auto delete

Facebook Container

Firefox Multi-Account Containers



Private

Secure

Ads blocks

HTTPS upgrading

Private window with TOR

ACCESSING WEBS SECURELY

Minimize browser leakage

1. Use a “private browsing” mode. This option is available with Firefox, Safari, Chrome.
2. Change your default search engine to something like DuckDuckGo or StartPage. These privacy-protecting search engines are noncommercial—they don’t track you or collect personal information or search history.

ACCESSING WEBS SECURELY

3. Clear your browsing history regularly. If your browsing history is stored in your browser (which in most browsers is the default), it can be collected by a variety of companies as you browse the web.

4. Opt out of Google and Apple showing you “personalized ads”: On Android you can find the opt-out in the Ads Settings; on iPhone, scroll down to the bottom of your Privacy settings to Advertising > Limit Ad Tracking.

<https://slate.com/technology/2017/02/cybersecurity-self-defense-how-to-increase-security-on-your-smartphone.html>

ACCESSING WEBS SECURELY

Consider using VPN

- Disguises your actual network IP address and encrypts internet traffic between a computer (or phone or any networked “smart” device) and a VPN’s server.
- Acts as a sort of tunnel for your internet traffic, preventing outsiders from monitoring or modifying your traffic. Traffic in the tunnel is encrypted and sent to your VPN, which makes it much harder for third parties like internet service providers (ISPs) or hackers on public Wi-Fi to snoop on a VPN users’ traffic or execute man-in-the-middle attacks.

ACCESSING WEBS SECURELY

Consider using VPN

- - Offers more privacy and security, but does not make you completely anonymous online: your traffic can still be visible to the operator of the VPN.
- - not the same thing as an ad blocker, does not, by default, disrupt other sorts of online tracking.
- Free VPN apps: Psiphon and Tunnelbear

ACCESSING WEBS SECURELY

TOR and VPN

- Tor is a free browser that provides maximum anonymity through a decentralized server network. It is best for transmitting highly-sensitive information, but it's extremely slow.
- There's the probability that exit nodes could read unencrypted data, but not the source of such data.

ONLINE SECURITY- EMAIL

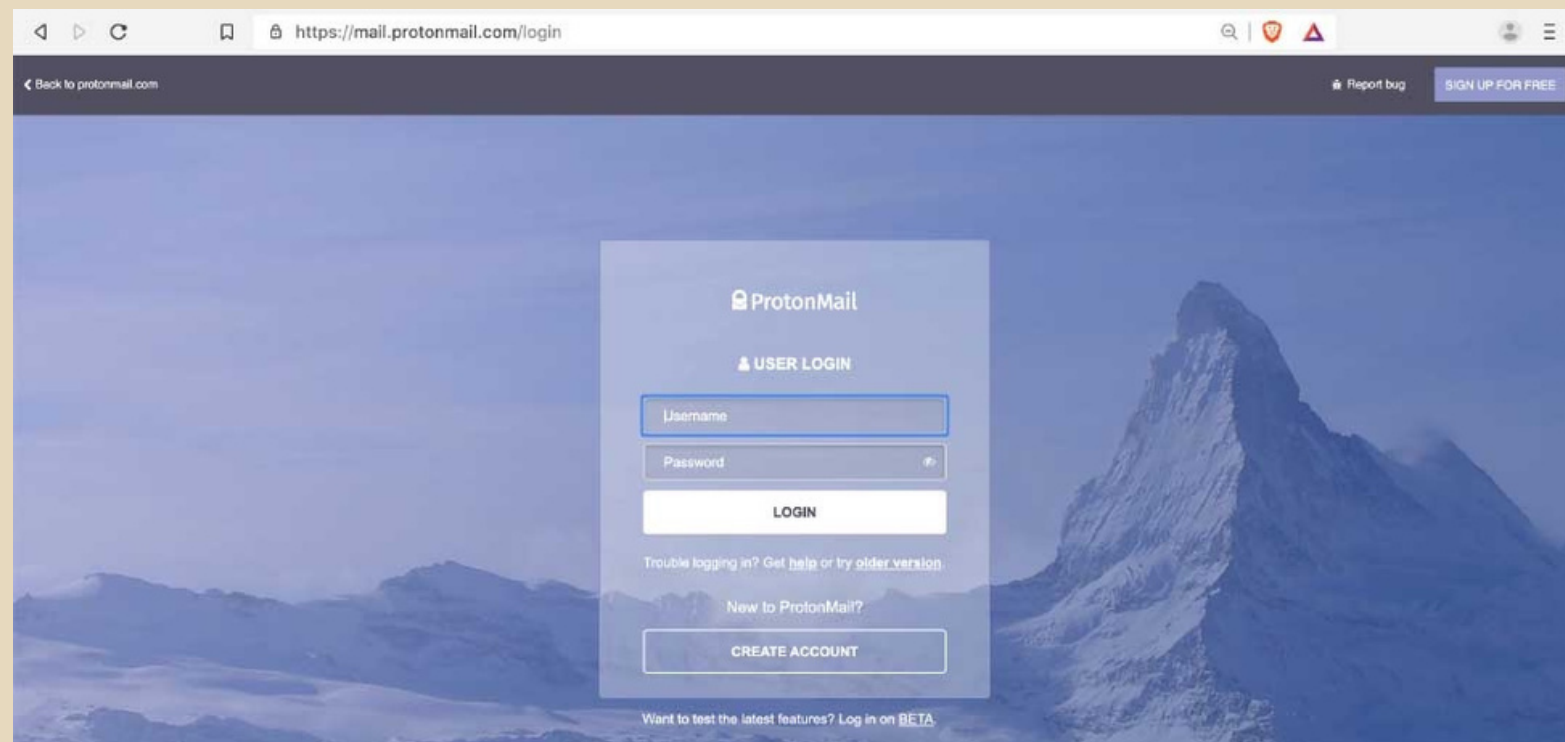
- All of the information contained in your inbox, your sent folder and your address book are only as secure as your digital security practices.

EMAIL



Google collects a lot of information about its Gmail users that can put you at risk. If you must use Gmail, read its privacy policy and understand the risks.

EMAIL



ProtonMail offers end-to-end encryption if you are sending an email to another ProtonMail account. Emails sent to recipients who do not have a ProtonMail account can also be encrypted with an added password that the recipient must know.

EMAIL

- Consider setting up multiple email accounts and using one or more as a decoy. Setting up new email accounts will make it more difficult to identify and monitor you.
- Make it difficult to link your identity to your email account(s).

EMAIL

- Don't open emails with suspicious subject lines; they may contain viruses or malware.
- Don't open attachments from email addresses that you don't recognize; they may contain viruses or malware.

PHISHING



Electronic equivalent of fraud

Take the quiz:

<https://phishingquiz.withgoogle.com/>

PROTECTION VS PHISHING

- Keep all your software updated (OS, apps, AV)
- Examine messages and emails and their content
- Look for spelling mistakes, errors and check facts
- Verify emails with senders

PROTECTION VS PHISHING

- Test URL and files in [virustotal.com](https://www.virustotal.com)
- Open suspicious files in Google Drive
- Use 2FA to protect your online accounts

MALWARE

Malware is what infects your PC. The word is a combination of “malicious” and “software,” and it refers to viruses of all kinds.

- From infected hardware (such as USB sticks)
- From unlicensed or cracked software (e.g., fake download sites)

MALWARE

- By clicking malicious links to download viruses (e.g., fake advertisements)
- By downloading them through malicious email attachments
- Through social engineering attacks (i.e., impersonation)
- By downloading them through scams on social networking sites.

PROTECTION VS MALWARE

- Keep your software and OS up to date
- Install and keep up to date an anti virus software
- Use password manager
- Do not use pirated software
- Install a Firewall that helps protect your device!