

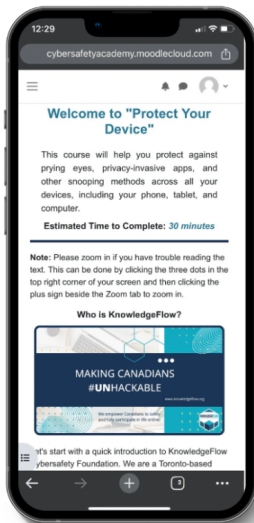
- Download your participant certificate and handouts
- Complete the survey

The screenshot shows the KnowledgeFlow.org website with a navigation bar including 'KNOWLEDGEFLOW', 'About Us', 'Resources', 'Initiatives', 'Solutions', 'Cyber Hub', 'Events', 'Blog', and 'Contact'. The main content area features an event titled 'Be #UnHackable - 4 Keys To Online Safety - Stouffville' on February 12 at 2:30 PM - 3:30 PM. Below the event title is a 'Join Us' section with text about acquiring insights from Claudiu Popa, a cybersecurity expert. There are two boxes at the bottom: 'Participant Materials' with a 'View Materials' button and 'Participant Survey' with an 'Open Survey' button.

## Access Our FREE Courses

KnowledgeFlow.org

The screenshot shows the website's navigation bar with 'Academy' highlighted by a red box and a yellow arrow pointing to it. The navigation bar includes 'KNOWLEDGEFLOW', 'About Us', 'Resources', 'Initiatives', 'Solutions', 'Cyber Hub', 'Academy', 'Events', 'Blog', and 'Contact'.



Course card for 'Protect Your Device' with a 'FREE' badge. The card features an icon of a smartphone and a laptop. The text reads: 'Protect Your Device', 'Cybersafety for Everyone', and 'FREE'.

Course card for 'Protect Your Information' with a 'FREE' badge. The card features an icon of a computer monitor with a person silhouette. The text reads: 'Protect Your Information', 'Cybersafety for Everyone', and 'FREE'.

Course card for 'Scams: Spot Them and Stop Them' with a 'FREE' badge. The card features an icon of a magnifying glass over an eye. The text reads: 'Scams: Spot Them and Stop Them', 'Cybersafety for Everyone', and 'FREE'.

Course card for '10 Immutable Rules of Cybersafety' with a 'FREE' badge. The card features a comic book-style graphic with the text 'CLAUDIU'S 10 IMMUTABLE RULES OF CYBERSAFETY'. The text reads: '10 Immutable Rules of Cybersafety', 'Cybersafety for Everyone', and 'FREE'.

Be  
Private

Be  
Secure

Be  
Skeptical

Be  
Positive

## Password Checklist

1



### UNIQUE

Create a different password for each account

2



### STRONG

Long, with capitals, numbers and characters

3



### SECURE

Store in a password manager

4

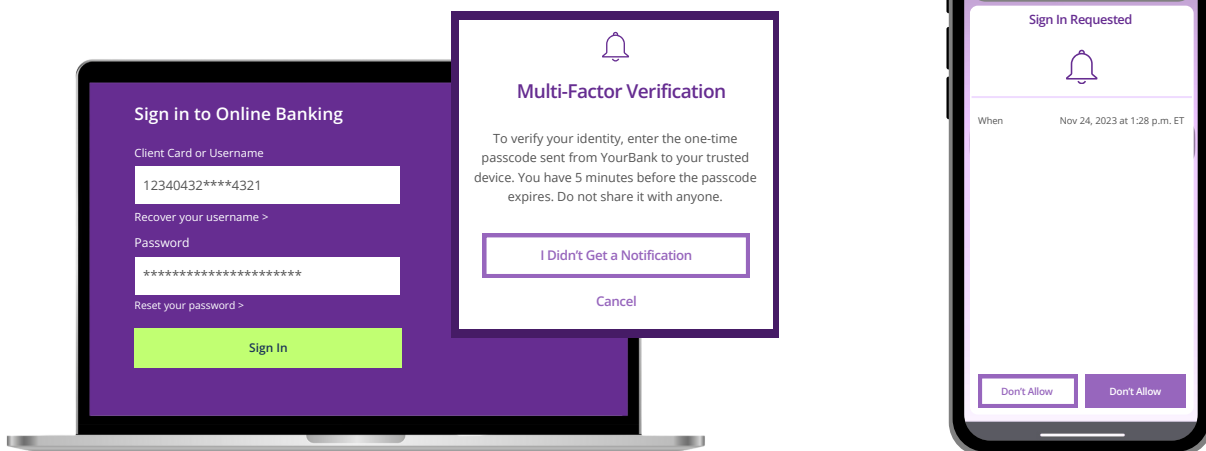


### COMPLEX

Enable multi-factor authentication

Enable MFA on **all accounts** that involve personal information and/or financial transactions

- Online bank accounts
- Social media accounts
- Shopping accounts
- Canada Revenue account

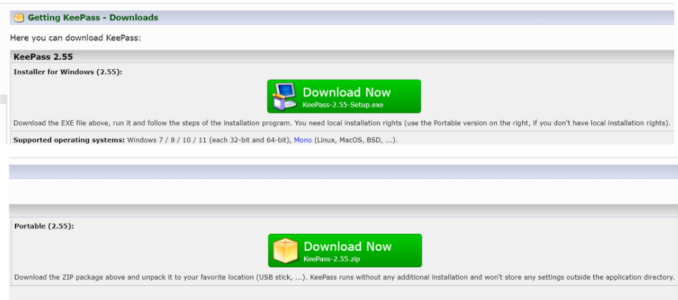


Consider changing providers if MFA is not offered.

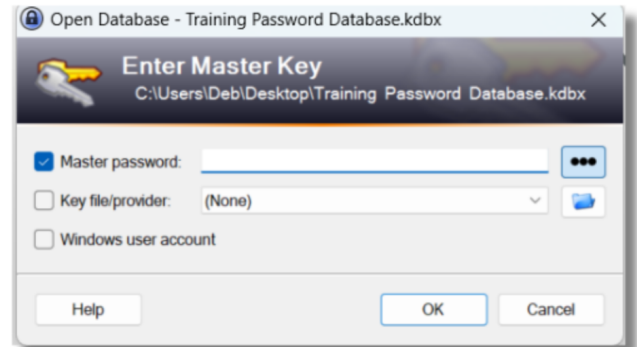
Password Manager - Example: KeePass

## KeePass.info

### 1. Download the program



### 2. Set your Master Password



- Use adblocking tools that run in your Web browser:

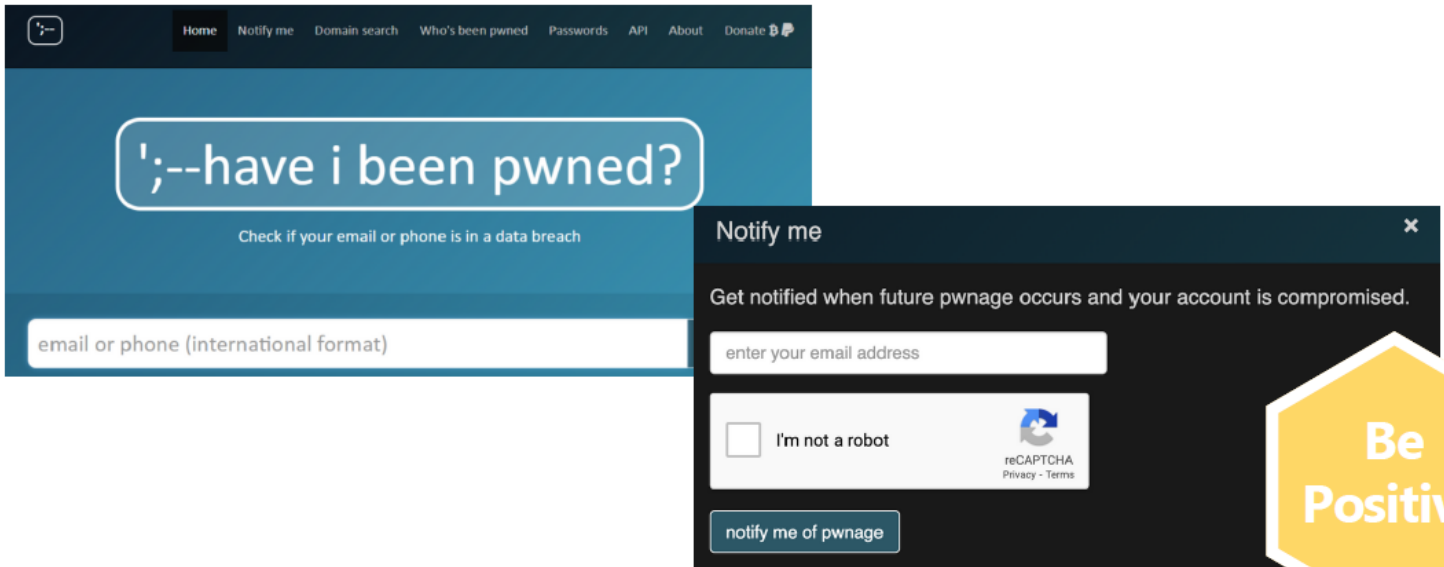


## AdblockPlus



## CleanBrowsing

## Get Notified

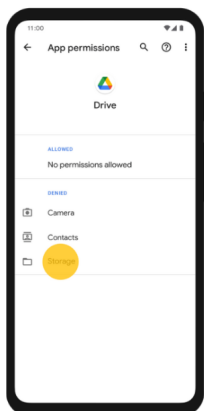


The screenshot shows the 'Have I Been Pwned' website interface. At the top, there's a navigation bar with links like 'Home', 'Notify me', 'Domain search', 'Who's been pwned', 'Passwords', 'API', 'About', and 'Donate'. The main heading is '';--have i been pwned?' with a subtext 'Check if your email or phone is in a data breach'. Below this is a search input field labeled 'email or phone (international format)'. A 'Notify me' modal is open, containing a form to 'enter your email address', a checkbox for 'I'm not a robot' with a reCAPTCHA logo, and a 'notify me of pwnage' button.



# How to be #UnHackable: Be Private

- Review your app permissions
- If a product or service is FREE = you may be the product



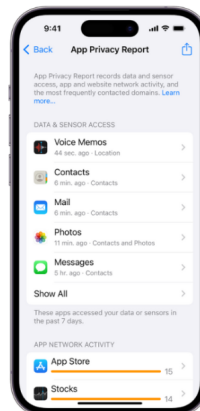
## Android

### Review or Change App Permissions

Touch and hold the app > App info > Permissions

Tap the permission you want to change

Choose Allow or Deny



## IOS

### Review or Change App Permissions

Go to Settings > Privacy & Security

Select a category such as Calendars

Turn access on or off

### Review how apps are using permissions

Go to Settings > Privacy & Security > App Privacy Report.



- Never feel pressured to pay or respond to urgent deadlines
- Watch for signs of fearmongering
- Ignore requests for secrecy, 'court gag orders', etc.
- Badge numbers, case numbers, employee numbers, logos, company names, department name - can all be made up
- Unexpected requests for payment, refunds, or to dispute charges are all the same - phishing
- Even if they already have some your info - like your name, address, phone number, SIN, health card number - doesn't mean they are legitimate
- Requests to provide or confirm your information are just as sketchy if you did not initiate the call