What can be done to prevent SIM swaps?

CBC | MENU | Paris 2024

10 arrested in SIM swap fraud investigation: Toronto police

Ethan Lang · CBC News · Posted: Aug 01, 2024 1:34 PM EDT | Last Updated: August 1

After a year-long investigation, Toronto police have arrested 10 people allegedly involved in a "SIM swap" fraud scheme, where criminals take over people's phone numbers in order to access personal information and bank accounts.

Over 1,500 cellular accounts across Canada were compromised by the scam, police said at a news conference Thursday.

The fraud cost victims, telecommunications companies and financial institutions over $1 million combined, police said.

- The news about SIM theft is quite scary
- Do you have any specific ideas on protection for this particular threat?

Bea [redacted]

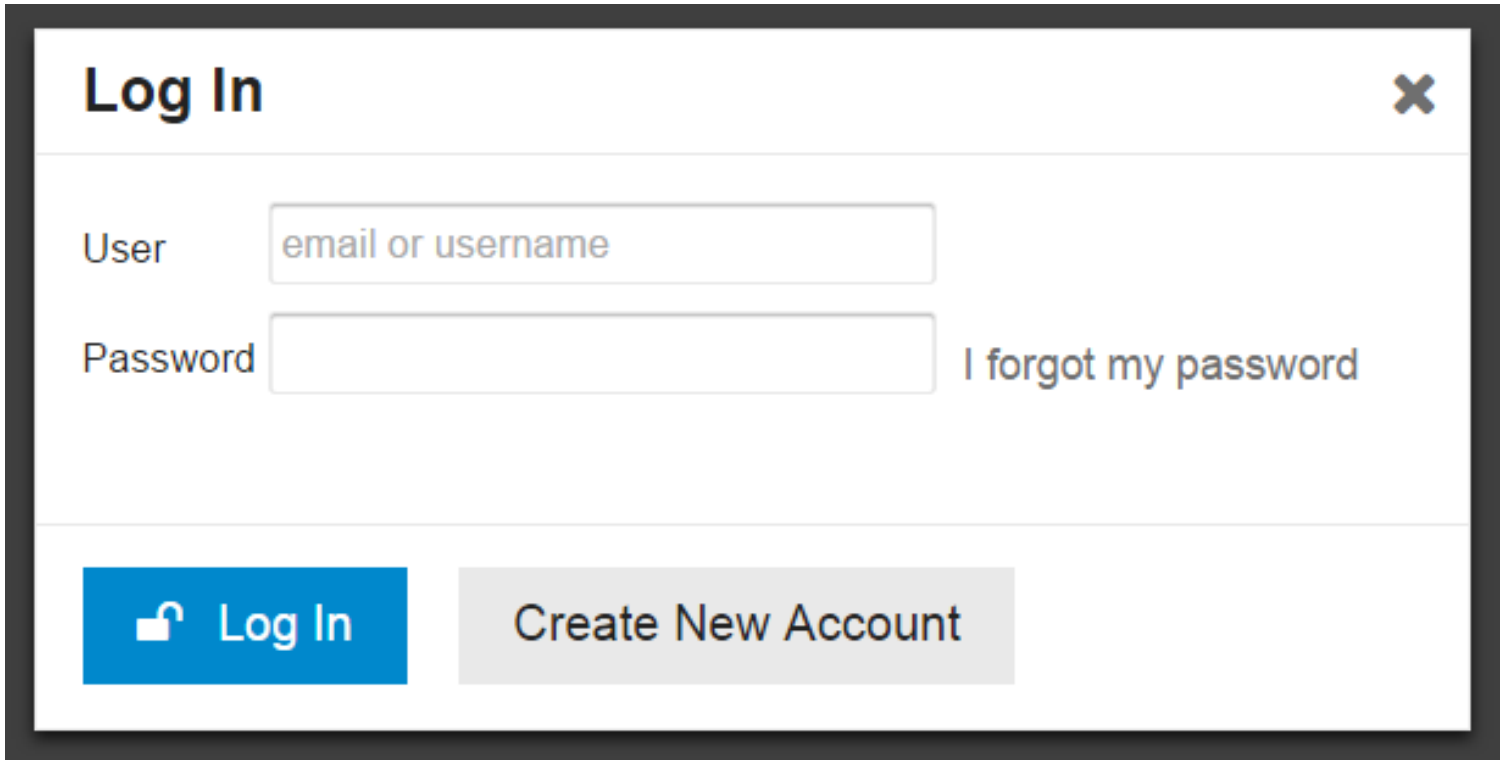
https://www.cbc.ca/news/canada/toronto/project-disrupt-sim-swap-arrests-1.7282288

What is a SIM swap?

- Scammer contacts your mobile phone carrier
  - tricks them into transferring your phone number to their SIM card
- Why or when is this a bad thing?
- A website **requires two factor authentication** (2nd factor: one-time code sent in a text message to your mobile)
  - scammer enters your username/password signing in to a service
  - service sends one-time code by text to your mobile number
    - which is now scammer's phone
  - scammer enters code at website & completes sign-in to your account
- How likely is this—or any—account compromise?
- Let's take a deep breath…step back… and discuss all types of authentication

Password-only authentication

- You are prompted to sign in
- You enter your username and password
- You are signed in



Password-only authentication Vulnerability one

- Someone guesses your credentials
  - or hacks the website, obtains encrypted password database and uses password cracking software to obtain plaintext passwords
- They can sign in as you
- Mitigation
  - use very long, unique passwords (preferably over 20 characters)
    - **use a password manager so you don't have to remember them all**
  - **don't** use dictionary words, common phrases, info about you, etc.
    - having a 20+ character password effectively eliminates these
  - **don't** give your password to anyone else, don't write it down where someone else might find it, etc.
  - if your email address has been found in data breaches
    - https://haveibeenpwned.com/
- Effectiveness of mitigations
  - very good

Password-only authentication Vulnerability two

- Website provides a way to reset your password by answering "security" questions
- If someone can guess the answers or research them, they can reset the password and sign in as you
- Mitigation
  - **use** nonsense answers to security questions
    - city where you grew up: *moonbeam*
    - mother's maiden name: *bookcase*
  - record answers in your password manager
- Effectiveness of mitigation
  - very good

Password-only authentication Vulnerability three

- Website provides a way to reset your password by sending a reset (usually a URL) to your email
- If someone gains access to your email account, they can:
  - request a password reset from original site
  - intercept the password reset email, reset the password, and obtain access to the original service
- Mitigation
  - protect access to your email more than other services
- Effectiveness of mitigation
  - good
    - depending on strength of protection added to email account

Password-only authentication Vulnerability four *(SIM swap)*

- Service allows password resets by sending a reset link to your mobile phone as text message
  - **this is not common**
- If someone can convince your mobile service provider to change your phone number to a SIM they own
  - can intercept password reset text message, reset password, & sign in as you
- Mitigation
  - **don't** enable password resets through text messaging
  - ask phone company to block moving phone number to a different phone unless you show up in person with photo ID
    - my phone service provider put a note on my file to this effect
  - if you ever can't access the mobile network, immediately contact your phone company (it might be too late)
- Effectiveness of mitigation
  - excellent

Password-only authentication Vulnerability five

- Attacker tricks you into going to a look-alike site (e.g. email phishing attack)
- You sign-in, giving credentials for real site to attacker
- Attacker goes to the real site and signs-in as you
- Mitigation
  - **enable** two-factor authentication
    - attacker then needs to compromise not only your username/password, but also your second factor
- Effectiveness of mitigation
  - very good
  - Google: after implementing two-factor authentication, successful phishing attacks on internal network dropped to zero

Two-factor authentication

- To authenticate
  - **must first provide a username and password**
  - second factor then required, either:
    - something you have, e.g.:
      - phone to receive a text message with one-time code
      - a security key you can plug into a USB port
    - something you are, e.g.:
      - fingerprint
      - facial recognition
      - iris scan
- ***Given password-only mitigations can be effective***
  - ***adding a second factor can only strengthen things***

Two-factor authentication Vulnerability one

- You lose control of "something you have"
  - someone who **already** knows your username and password **and** gains control of "something you have" can sign on as you
- Keep in mind, if "something you have" is your phone
  - good chance there is lots of info on it identifying services you use, usernames (often email addresses) etc. that can help an attacker
- Mitigation
  - secure "something you have" carefully
  - if "something you have" is your phone, secure it very well
- Effectiveness of mitigation
  - okay to very good
    - depending on how well you secure "something you have"

Two-factor authentication Vulnerability two *(SIM swap)*

- If your second factor is a one-time code sent in text message to your mobile
  - someone who **already** knows your username and password **and**
  - has your phone number transferred to a phone they own
  - can intercept text message with one-time code and sign on as you
- Mitigation one
  - ask phone company to block moving phone number to a different phone unless you show up in person with photo ID
    - my phone service provider put a note on my file to this effect
  - if you ever can't access the mobile network, **immediately** contact your phone company (but it might be too late)
- Effectiveness of mitigation
  - very good
    - as long as you protect your phone very well

Two-factor authentication Vulnerability two *(SIM swap)*

- If your second factor is a one-time code sent in text message to your mobile
  - someone who **already** knows your username and password **and**
  - has your phone number transferred to a phone they own
  - can intercept text message with one-time code and sign on as you
- Mitigation two
  - if the service supports use of *authentication app*
  - switch from text message to an authentication app for second factor
    - **text message** is tied to your **phone number**
      - vulnerable to SIM swaps
    - **authentication app** is tied to **your phone**
      - not vulnerable to SIM swaps
- Effectiveness of mitigation
  - very good to excellent
    - depending on how well you protect your phone

Two-factor authentication Vulnerability three

- Phishing attack sends you to a look-alike site
  - attacker is watching your inputs in real-time
  - you enter your username & password
  - when prompted, you enter your one-time code
    - ***whether from a text message or an authentication app***
  - attacker goes to real site
  - enters your username, password, and one-time code
- Can also happen through capture of session cookies
  - how a website knows it is still you while navigating site
- Mitigation
  - if a site requires authentication
    - never, **never**, ***never*** follow a link sent to you via email, text, etc.
    - **only** access websites requiring authentication through a trusted source
- Effectiveness of mitigation
  - very good

Summary & cautions

- ***Any*** two-factor authentication ***much*** stronger than single factor
  - *be sure to also follow mitigations for password-only authentication*
- Authentication apps mitigate more risks than codes sent via text messages
  - mitigates SIM swap vulnerability
  - doesn't mitigate vulnerability of attacker collecting username, password, ***and*** one-time code
- Even two-factor authentication **can** be defeated
- **There is no such thing as perfect security**
  - ***The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts***
    - **Gene Spafford, computer security expert, Perdue University**

Summary & cautions

- With passwords, length trumps complexity
  - **`BlueSkiesAreFallingDown`**
    - 23-character non-complex password is **79 times stronger** than
  - **`OrCfPEK~vjG9Aq!18cd`**
    - 19-character complex password
  - **`5555+5555+5555+5555+5555`**
    - *24-character password that is very strong*
- If service permits multiple means of password recovery
  - weakest means always trumps stronger means, e.g.
    - if you can use either an authentication app or an email message with a one-time code,
    - the email message with a code will likely be used by attacker

Summary & cautions

- Think about digital legacy
  - can anyone handle your accounts in case of incapacity/death?
- Highest protection should be given to highest-valued services, e.g.
  - bank accounts
  - services with highly-sensitive information
  - email accounts used for password recovery & two factor authentication
- **The strongest means of authentication is also the most likely to cause accidental lock-out from a service!**
  - think about what happens if your second factor is unavailable

Resources

- Password manager
  - allows for easy use of very long and complex passwords, recording of nonsense “security” questions, & any other sensitive data
  - https://opcug.ca/Reviews/ProtectPasswords.html
  - https://opcug.ca/Reviews/KeePass.htm
  - https://opcug.ca/presentations/keeping-passwords-safe.pdf
- https://haveibeenpwned.com/
  - excellent free service
  - find out if your email address has shown up in a data breach
- How big is your haystack?
  - https://www.grc.com/haystack.htm
- Ottawa Public Library presentation: ***Keeping passwords safe***
  - Thursday, October 10, 6pm, Alta Vista
  - Tuesday, October 22, 2pm, Ruth E Dickinson

Defeating two-factor authentication

- https://www.itworldcanada.com/article/google-users-say-two-factor-authentication-didnt-protect-them-hashtag-trending-for-monday-april-15th/560424
- https://www.itsolutions-inc.com/blog/articles/new-phishing-attacks-make-2fa-useless-updated/