

Is Your Account Really Being “Hacked”?

Here's How to Protect Yourself Online



When people hear an account was "hacked," they often imagine a cybercriminal breaking through advanced security systems. In reality, most account compromises happen when someone is tricked into sharing login information or relies on weak security practices.

The good news? A few simple habits can significantly reduce your risk.

1

NEVER SHARE PASSWORDS, PINs, ACCOUNT NUMBERS, SOCIAL SECURITY NUMBERS, SECURITY CODES OR ANY OTHER IDENTIFIABLE INFORMATION

First Peoples will never call you to request any of this information. If someone does call, hang up and call our official phone number: **1-301-784-3000 or 1-800-655-8335.**

2

USE STRONG, UNIQUE PASSWORDS

Your password is your first line of defense.

Passwords that are long and complex are exponentially more difficult to guess. Security experts recommend using passwordss that are at least 15 characters long when multi-factor authentication (MFA) isn't enabled, or at least 8 characters when MFA is required.

A few tips:

- Avoid using names, birthdays, addresses or other personal information.
- Use a passphrase, such as a memorable sentence or a series of unrelated words.
- Use a different password for every account. If one account is compromised, the others remain protected.
- Consider a password manager to generate and securely store strong passwordss.
- Learn more about strengthening your passwordss at www.firstpeoples.com/strong-passwords.

3

TURN ON MULTI-FACTOR AUTHENTICATION (MFA)

MFA adds an extra layer of security beyond your password. Even if someone obtains your password, they'll still need a second verification method to access your account.

Whenever MFA is available, enable it.

Most importantly: **Never share an MFA code** with anyone. Legitimate businesses will never call, text or email asking for your verification codes.

Learn more about MFA at www.firstpeoples.com/mfa.

4

USE PASSKEYS WHEN AVAILABLE

Passkeys are becoming a safer and more convenient alternative to traditional passwordss.

Instead of memorizing a password, you sign in using your device's built-in security features, such as:

- Fingerprint recognition
- Face ID
- Device PIN
- Passkeys: Because there is no password to steal, passkeys are highly resistant to phishing attacks. Learn more about Passkeys at www.firstpeoples.com/passkeys.

5

MONITOR YOUR ACCOUNTS REGULARLY

Checking your account balance is important, but it's equally important to review your recent transactions.

Look for:

- Purchases you don't recognize
- Unexpected transfers
- Changes to your account information

The sooner suspicious activity is detected, the sooner it can be reported and addressed.

6

SET UP ACCOUNT ALERTS

Account alerts can help you identify unusual activity quickly. Consider enabling:

Security Alerts

– Notifications when:

- Someone attempts to log in from a new device
- Multiple failed login attempts occur
- Account information is changed

Transaction Alerts

– Notifications when:

- Purchases exceed a selected dollar amount
- Account balances fall below a threshold
- Transfers or withdrawals occur

Unexpected alerts can be an early warning sign that something isn't right.

7

REPORT SUSPICIOUS ACTIVITY

Act quickly: Report suspicious account activity or unfamiliar transactions as soon as you notice them. Prompt reporting can help secure your account and stop fraud before it spreads.

8

BE CAREFUL ABOUT WHAT YOU SHARE ONLINE

Scammers often gather information from social media profiles and public websites.

Scammers may use publicly shared details to guess passwordss or make fraudulent messages seem more believable. Be especially cautious about sharing:

- Birthdays
- Family members' names
- Pet names
- Favorite sports teams
- Schools attended

Even small personal details can be valuable to criminals when they are trying to access your accounts or target you with scams.

Is Your Account Really Being “Hacked”?

Here's How to Protect Yourself Online



9

LEARN TO RECOGNIZE PHISHING SCAMS

Phishing remains one of the most common ways criminals gain access to accounts.

Phishing occurs when someone uses email, text messages, phone calls or fake websites to trick you into revealing sensitive information.

Common warning signs include:

- Urgent requests demanding immediate action
- Unexpected login or verification requests
- Suspicious links or attachments
- Messages that create fear or panic

When in doubt, contact the company directly using a phone number or website you know is legitimate. Learn more about Phishing at www.firstpeoples.com/phishing.

10

VERIFY WEBSITES BEFORE CLICKING

Before clicking links in emails or text messages, inspect them carefully.

A safer approach is to:

- Open your web browser
- Manually type the website address
- Log in from the official website

This simple habit can help prevent you from landing on a fake site designed to steal your credentials.

11

DOWNLOAD APPS ONLY FROM TRUSTED SOURCES

Unofficial app stores and "free software" websites can contain malicious programs designed to steal personal information.

To stay safe:

- Download apps only from the Apple® App Store® or the Google Play™ store.
- Avoid software from unknown websites.
- Be cautious of apps with poor reviews or limited download history.

12

REVIEW APP PERMISSIONS

Many apps request access to information on your device, including:

- Photos
- Camera
- Contacts
- Location

Take time to review permissions periodically and disable anything that isn't necessary.

Ask yourself: Does this app truly need access to this information?

If not, turn it off.

13

KEEP YOUR DEVICES UPDATED

Software updates do more than add new features—they often contain important security fixes.

Enable automatic updates whenever possible for:

- Operating systems
- Web browsers
- Mobile devices
- Apps

Keeping software current helps protect against known vulnerabilities.

Please Note: Windows 10 and everything that came before it is no longer getting these important security updates. Maybe it's time to upgrade!

14

USE ANTIVIRUS AND MALWARE PROTECTION

Security software can help detect and block malicious programs before they cause damage.

For best protection:

- Keep security software updated.
- Enable real-time protection features.
- Run regular scans.

Security software isn't a replacement for safe online habits, but it adds another valuable layer of protection.

15

BE CAREFUL WITH PUBLIC WI-FI

Public Wi-Fi networks can be convenient, but they also present risks.

Avoid accessing sensitive information such as:

- Online banking
- Financial accounts
- Medical records
- Shopping accounts containing payment information

When possible, use your cellular connection or a trusted network instead

STAY VIGILANT

Online security doesn't require technical expertise—it requires awareness and good habits.

By using strong passwords, enabling MFA, recognizing phishing attempts, monitoring your accounts and keeping your devices updated, you can greatly reduce the chances of becoming a victim of fraud.

Remember: Most account compromises don't happen because a criminal "hacked" their way in. They happen because someone was tricked into opening the door. A little caution goes a long way toward keeping your information safe.