

The 10 Cyber Commandments



Most online theft starts with a stolen password, a fake message or an "urgent" call. These ten habits close those doors.

I Thou shalt turn on multi-factor authentication.

Use a passkey where offered, or an authenticator app or security key; text codes are the weakest option. Start with email and banking. In a Microsoft study, MFA cut account-takeover risk by over 99%.

II Thou shalt use a password manager.

A long, different password for every account. Pick a reputable one, such as 1Password, Bitwarden or the one built into your phone or browser.*

III Thou shalt freeze thy credit at all three bureaus.

Equifax, Experian and TransUnion. It's free, doesn't affect your score, and blocks new accounts in your name.

IV Thou shalt guard thy email like the master key.

Every password reset lands there. Give it a unique password, a passkey or app-based MFA, and current recovery details.

V Thou shalt verify before thou trustest.

Unexpected urgency? Hang up and call back on a number you look up yourself. **Imposter scams were the most-reported fraud of 2025**, nearly 1 in 3 fraud reports to the FTC.

VI Thou shalt not pay by gift card, crypto or wire on demand.

No government agency or real business demands it. And your bank will never ask you to move money to "keep it safe."

VII Thou shalt not click unexpected links or attachments.

Email, texts, QR codes, direct messages: even if it looks like your bank or the IRS, go to the real site or app yourself.

VIII Thou shalt turn on automatic updates.

Attackers lean on known flaws that already have a fix. Replace devices that no longer get updates.

IX Thou shalt back up what thou canst not bear to lose.

Keep one copy offline or in a cloud backup with version history, and test a restore. It's your undo button for ransomware.

X Thou shalt not overshare.

Birthdays, pet names and travel plans feed password guesses and scams. Voices can be cloned: agree on a family code word.

If thou doest only three things: turn on MFA, get a password manager, freeze thy credit.

Together they stop the most common account takeovers and block new credit in your name.

Scammed or targeted? Report it at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov), and online crime at ic3.gov. It helps stop them for the next person.

* Examples, not endorsements. **Sources** (checked October 2026): FTC Consumer Sentinel 2025 data, credit freeze and gift card guidance; CISA Secure Our World and mobile communications guidance; NIST SP 800-63B-4; Microsoft MFA research (2023); FBI PSA I-120324-PSA; Verizon 2026 DBIR.

