INSTITUTE FOR HOUSEHOLD CYBERSECURITY

The IHCS Standard v0.1

Competency areas for the HCA™ Personal certification. Summary edition, October 2026.

Purpose

This Standard defines the knowledge and habits a head of household needs to protect the people in their home from modern scams and account takeover, especially threats enabled by artificial intelligence. HCA™ Personal certifies an individual against this Standard for their own household.

Competency areas

AREA 1 **AI-enabled impersonation**	Recognize voice clones, deepfake video and synthetic messages. Understand why perception alone is no longer a reliable test of identity.
AREA 2 **Phishing, smishing & vishing**	Understand how manipulation works across email, text and phone, including urgency, authority and secrecy, and apply response habits that defeat it.
AREA 3 **Verification protocols**	Establish a family code word, callback rules using known numbers, and a pause-before-paying practice for every adult in the home.
AREA 4 **Accounts & identity**	Use a password manager and multi-factor authentication, secure account recovery paths, and know when and how to freeze credit.
AREA 5 **Devices & home network**	Apply sensible defaults to phones, computers, routers and connected devices: updates, screen locks and router administration.
AREA 6 **Protecting kids & aging parents**	Recognize threats specific to children, teens and older adults, and teach household protocols in a way each group will actually use.

How the Standard is maintained

The Standard is published openly and versioned. Each certificate records the version it was earned against. The Institute is independent and the Standard does not require any particular vendor, product or app.

Limits

This Standard is educational. Meeting it makes a household a harder target. It does not guarantee protection against every threat.

© 2026 Institute for Household Cybersecurity. HCA™ is a trademark of the Institute for Household Cybersecurity. May be shared for personal, non-commercial use with attribution.