Complaint Summary:

Family member was targeted by two separate online scams.

Advance Fee / Fraud Scam – $300 USD:

On August 11, 2025, she encountered a fraudulent “government empowerment program” via a YouTube link. Believing it to be legitimate, she submitted her personal information and paid $300 USD. Shortly afterward, we realized it was a scam. Documentation of the payment is available.

Extortion / Email Scam – $500 USD:

On September 13,2025, she received an email sent from what appeared to be her own email address (xxxx). The sender claimed to have hacked her email and computer, alleging they had recorded her through her webcam and threatening to release sexually explicit videos unless she sent $500 USD in Bitcoin. The email included a Bitcoin wallet address and payment instructions. This was a spoofed email; no devices were actually compromised, and no such videos exist. No payment was made.

Immediate Response:

- Changed account password
- Removed unauthorized linked emails and phone numbers
- Enabled recovery options (MFA via phone, Microsoft Authenticator, email code)
- Installed antivirus / antimalware / anti-spam on devices

Evidence available: Screenshots of emails, header information, and payment confirmation for the $300 scam.