Fake LastPass Death Claims Used to Breach Password Vaults

A phishing campaign tied to the financially motivated group CryptoChameleon (UNC5356) is targeting LastPass users with fake "legacy access" emails claiming that a relative submitted a death certificate to access their vault.

The campaign tricks victims into entering their master password or passkey on spoofed sites like lastpassrecovery[.]com and mypasskey[.]info. Some victims have also received phone calls from attackers impersonating LastPass staff.

Overview

LastPass has issued a warning about an ongoing phishing campaign that began in mid-October 2025. Attackers are sending fraudulent emails from spoofed addresses such as alerts@lastpass[.]com, using the subject line "Legacy Request Opened (URGENT IF YOU ARE NOT DECEASED)." The message falsely claims that a family member uploaded a death certificate to initiate an emergency access request, prompting recipients to "cancel" the request via a malicious link.

That link redirects victims to lastpassrecovery[.]com, a convincing fake login portal designed to steal LastPass master passwords. In some cases, the attackers have followed up with phone calls. They pretend to be LastPass representatives and urge victims to verify their accounts.

Threat Actor

Google Threat Intelligence has attributed this campaign to CryptoChameleon, also tracked as UNC5356. The group is financially motivated and is known for stealing cryptocurrency via advanced phishing kits. UNC5356 uses bulletproof hosting infrastructure, often through NICENIC, and has previously targeted users of Coinbase, Binance, Gemini, Kraken, and Uphold, as well as platforms like Okta, Gmail, and Outlook.

CryptoChameleon's reuse of LastPass branding isn't new. The same group ran a similar campaign in April 2024, but the current one shows broader reach and technical upgrades, including the ability to target passkey credentials. Organizations relying on password managers should verify that staff understand what legitimate inheritance requests look like and know never to enter credentials outside the official LastPass domain (lastpass.com).

Aspire Protects

- Do not trust inheritance or death-related access requests. Legitimate requests are visible only inside the LastPass interface, not via email links.
    - A real Emergency Access (legacy) request is started and visible inside LastPass by a trusted contact who was pre-approved in your vault. It follows a preset waiting period and never requires you to type your master password into a link from an email or on a phone call. Take a look at some red flags:
        - Any email or SMS that asks you to click a link to “cancel” or “verify” a legacy request that leads to a non-LastPass domain (anything other than lastpass.com).
        - Messages that demand urgent action (“URGENT IF YOU ARE NOT DECEASED”) or include one-off agent/case IDs designed to create panic.
        - A caller claiming to be LastPass support who asks you to enter your master password on a site or over the phone.
        - Links with domains like lastpassrecovery[.]com, passkeysetup[.]com, mypasskey[.]info, or other suspicious domains — these are indicators of phishing. (If you see them, do not click.)
- Verify URLs before logging in. The only legitimate domain is lastpass.com.
- Enable MFA for both LastPass and associated email accounts.
- Report suspicious emails or calls to abuse@lastpass.com
- Train employees on hybrid phishing-and-voice social engineering tactics.
- Monitor for credential re-use across business systems if LastPass credentials are compromised.

TTPs to Watch

Initial Access

- Phishing: Spearphishing Link [T1566.002] – Attackers may distribute convincing inheritance-themed emails to lure users into clicking malicious links.

Credential Access

- Input Capture [T1056] – The phishing site may collect master passwords entered by victims.
- Modify Authentication Process [T1556] - Attackers may attempt to intercept or manipulate authentication flows for FIDO2/WebAuthn passkeys by spoofing legitimate passkey setup domains (e.g., mypasskey[.]info, passkeysetup[.]com).

Impersonation

- Social Engineering [T1656] – Threat actors may call victims directly, pretending to be LastPass representatives to reinforce trust and urgency.

IoCs

Domain

- lastpassrecovery[.]com
- mypasskey[.]info
- passkeysetup[.]com
- Numerous subdomains spoofing Coinbase, Binance, Gemini, and Google services

IPs

- 82[.]27[.]2[.]198
- 31[.]59[.]58[.]163

Targeted Industries

This phishing campaign threatens any organization that uses password managers for account authentication and credential storage.

- Education
- Public Sector
- Finance
- Healthcare
- Legal
- Manufacturing
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced

platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Possible CryptoChameleon Social Engineering Campaign Targeting LastPass Customers, Crypto Exchange Customers, Passkeys, and More