Cyber War:
Spam Bots Using Vietnamese, Chinese, and Russian Languages Selling “Insurance.”

Brand-impersonation phishing and malicious advertising risk.

The main cyber risks are:

- **Phishing:** The emails imitate Fidelity Life and eCoverage but were sent from unrelated domains.
- **Credential or identity theft:** “View Your Offer” may lead to a form requesting your name, address, birth date, Social Security number, income, medical history, or payment information.
- **Lead-generation fraud:** Your information could be collected and sold to insurance marketers, scammers, or data brokers.
- **Malicious links:** The buttons and unsubscribe links could redirect through tracking services, fake websites, or malware-delivery pages.
- **Email tracking:** Opening the message may load a tracking pixel that confirms your address is active and records your IP address, device type, and approximate location.
- **Domain abuse:** Legitimate but unrelated domains may have been spoofed, compromised, or used through insecure mailing accounts.
- **Conversation hijacking:** The “RE:” subject line creates the false appearance of an earlier conversation.
- **Inbox-filter evasion:** Garbled names, Chinese characters, unusual domains, BCC delivery, and modified subject lines can help bulk mail evade spam filters.

Overall risk: Hi**ghly suspicious spam with a meaningful phishing and personal-data risk.**

Do not click any buttons, attachments, or “unsubscribe” links. Report the messages as phishing, block the senders, and delete them. If you already entered information, change any affected passwords, enable multifactor authentication, monitor financial accounts, and consider freezing your credit. Simply viewing the email is usually much less dangerous than clicking a link, downloading something, or submitting information.

→ **Report Spam, Block Spam.**

All together, the emails mention or use the following companies and domains:

Company or domain	Apparent origin	Role
Fidelity Life Association	Chicago, Illinois, USA	Legitimate life-insurance company advertised in the messages. Its official domain is `fidelitylife.com`.
eCoverage	Bellevue, Washington, USA	Legitimate insurance-quote and marketing company named in the advertisement. Its official domain is `ecoverage.com`.
Zan BrandPack — `zanbrandpack.com`	Zambia	A Zambian sampling and brand-marketing company. Its domain appeared in one sender address.
`alexanorthstation.com`	Unknown	Unrelated sender domain. I could not verify a corresponding company or country.
`ibin.gxqzc.com`	Unknown	Unrelated and suspicious-looking sender subdomain. I could not identify a legitimate company behind it.

So, the advertised companies are American—**Fidelity Life in Illinois and eCoverage in Washington**—but the emails were transmitted using unrelated domains, including one associated with **Zan BrandPack in Zambia**. The Chinese characters and Gmail's Vietnamese-language warning suggest foreign-generated mailing data, but they do not establish China or Vietnam as the senders' locations.

Most importantly, none of the visible messages came from the official `fidelitylife.com` or `ecoverage.com` domains. Fidelity Life's official website ↗ and eCoverage's official website ↗ confirm their genuine domains.