Top 5 Cybersecurity Risks After Hurricane Helene

1. Impersonation Scams

Scammers pose as officials from FEMA or other organizations, requesting personal information or fees for expedited aid. Always verify the identity of any individual claiming to be an official by calling the FEMA helpline at 1-800-621-3362 to verify the person's identity.

2. Phishing Emails

Cybercriminals send fake emails claiming to provide disaster relief updates or donation opportunities. Avoid clicking on links or downloading attachments from unknown sources.

3. Fraudulent Charity Websites

Fake websites mimic legitimate charities to steal donations or collect sensitive information. Verify a charity's legitimacy before donating.

4. AI-generated social media posts

Scammers looking to exploit the emotions of those affected by Hurricane Helene by producing dramatic images intended to incite an emotional response and spread misinformation.

5. Data Breaches from Relief Applications

Applications for disaster relief might expose personal data if not handled securely. Only submit applications on official, secure websites.

Cybersecurity Do's and Don'ts

Do's:

- Verify the identity of anyone requesting personal information.
- Use official websites for disaster relief applications.
- Research charities thoroughly before donating.

- Enable two-factor authentication on your accounts.

- Report suspicious activities to authorities.

Don'ts:

- Don't click on links or download attachments from unknown emails.

- Don't provide sensitive information over the phone or email unless verified.

- Don't trust unsolicited offers for repairs or services.

- Don't use unofficial or insecure websites for transactions.

- Don't ignore warning signs of scams or fraudulent activities.