OFICINA DEL
COMISIONADO DE SEGUROS
GOBIERNO DE PUERTO RICO

PREPARING CITIZENS FOR CYBER RISKS

Recommendations from the **Office of the Commissioner of Insurance of Puerto Rico**

Message to Citizens

Information, prevention, and safe habits are your best protection in the digital environment.

OFICINA DEL
COMISIONADO DE SEGUROS
GOBIERNO DE PUERTO RICO

Message to Citizens

- Use **strong and unique passwords** for your most important accounts.
- Enable **multi-factor authentication (MFA)** whenever available.
- Keep your phones, computers, and applications **updated**.
- **Be cautious** of emails, text messages, or phone calls requesting personal or financial information.
- Carefully **verify** links before clicking on them or downloading files.
- **Avoid** using public internet networks for financial transactions or accessing confidential information.
- **Protect** the personal and financial information you share on social media.

Small actions today can prevent major problems tomorrow. Protect yourself and safeguard what is yours.

OFICINA DEL
COMISIONADO DE SEGUROS
GOBIERNO DE PUERTO RICO

Message to Citizens

- Make regular **backups of important** documents and photographs.
- **Regularly monitor** your bank accounts, credit cards, and credit reports.
- Immediately **report** any suspicious activity to your financial institution or service provider.
- Consider **financial protection** options and specialized cyber risk insurance when appropriate.
- **Prevention** and **education** are the most effective tools for reducing the risk of fraud and identity theft.
- **Cybersecurity** begins with informed decisions and safe habits.

Staying informed and taking precautions is the best defense against cyber threats.

OFICINA DEL
COMISIONADO DE SEGUROS
GOBIERNO DE PUERTO RICO

What should you do if you're a victim of a cyber incident?

- **Contact** your financial institution, insurance company, service provider, or affected platform **immediately**.
- If you have an insurance **policy** that may provide protection or assistance related to the incident, contact your insurance producer or authorized representative to learn about available coverages, benefits, and services under your policy.
- **Change your passwords** and enable multi-factor authentication (MFA) on affected accounts.
- **Preserve evidence** of the incident, including emails, messages, screenshots, and any other relevant information.
- **Monitor** your bank **accounts**, credit cards, and credit reports for suspicious activity.
- **Report the incident** to the appropriate authorities, including the Cybersecurity & Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) through the Internet Crime Complaint Center (IC3), and local authorities when appropriate.
- If your personal, financial, or medical information has been compromised, **act promptly** to limit potential damage and protect your identity.
- **Do not send money**, make payments, or share additional information with individuals or organizations whose legitimacy has not been verified.
- **Responding quickly** to an incident can be critical to reducing losses and protecting your personal and financial information.

https://myservices.cisa.gov/irf
https://www.ic3.gov