1. BDO should implement multi-factor authentication (MFA) to prevent unauthorized account access, especially when suspicious login locations or devices are detected. To combat phishing sites like "SCAMPAGE," they can deploy anti-phishing and domain monitoring technologies that detect and take down fake banking websites. Additionally, using behavioral analytics and AI-based fraud detection can identify unusual transaction patterns, such as sudden transfers to unknown accounts like "Mark Nagoyo," and temporarily block transactions until verified by the user through a secondary channel.

2. Bank users should enable multi-factor authentication (MFA) on all their financial accounts to add an extra layer of security beyond passwords. They should also use password managers to create and store strong, unique passwords for each banking site, reducing the risk of credential theft. Installing reputable anti-phishing browser extensions or security software can help detect and block fake banking sites, preventing them from accidentally entering login details on phishing pages like the GCash "SCAMPAGE."

3. Cybersecurity technologies play a critical role in protecting both financial institutions and customers from evolving threats. They help prevent unauthorized access, detect fraudulent activities in real-time, and mitigate damage before it escalates. In situations like the BDO hack, these technologies not only safeguard sensitive financial data but also help maintain public trust in digital banking systems. Without them, both banks and users would be highly vulnerable to well-organized cybercriminal activities.