FRAUD AWARENESS

Social Media Scams

Over the years, Facebook has been targeted by various scams. Here are some of the top scams that have been observed on the platform:

Phishing Scams: Scammers create fake Facebook login pages or send deceptive messages, trying to trick users into revealing their login credentials. These scams may appear as notifications, emails, or direct messages, claiming that there is an issue with the user's account and requesting their personal information.

Impersonation Scams: Scammers create fake Facebook profiles that impersonate well-known individuals, celebrities, or even friends. They use these fake profiles to engage in fraudulent activities such as requesting money, soliciting personal information, or spreading malware.

Fake Giveaways: Scammers create posts or pages on Facebook offering giveaways or prizes in exchange for liking, sharing, or commenting on their content. These scams aim to collect personal information, increase engagement, or redirect users to malicious websites.

Advance Fee Fraud: Scammers contact users through Facebook, claiming to have a large sum of money or valuable items that they are willing to share but require an upfront fee or payment for processing or other reasons.

Romance Scams: Scammers create fake profiles, often pretending to be interested in romantic relationships. They build trust with their targets and eventually request money for various reasons, such as travel expenses or medical emergencies, but disappear once the funds are sent.

How to protect yourself from these scams:

- ✓ Be cautious of messages or posts from unfamiliar or suspicious sources. Avoid clicking on suspicious links or downloading files from unknown sources.
- ✓ Verify the authenticity of pages by looking for verified badges, checking the account's history and content, and comparing it to official sources if applicable.
- ✓ Be skeptical of requests for personal information or financial transactions. Avoid sharing sensitive info with unknown individuals or unverified sources.
- ✓ Enable two-factor authentication (2FA) on your Facebook account for an added layer of security.
- ✓ Regularly review and adjust your privacy and security settings on Facebook to control who can see your posts, personal information, and friend requests.
- ✓ Keep your computer and mobile devices updated with the latest security patches and antivirus software to protect against malware and other threats.

If you encounter a scam on Facebook, report it to Facebook through their reporting tools or contact their support. Additionally, be sure to educate yourself about current scams and stay informed about security best practices to protect yourself and others on the platform.

BankFinancial℠

1.800.894.6900 | BankFinancial.com

Member FDIC