17 July 2026 **FEATURE ARTICLE**

The Scam Economy: Why Fiji Must Stay One Step Ahead

Scams are no longer isolated incidents carried out by opportunistic fraudsters. Today, they have evolved into a sophisticated global industry, often referred to as the **"Scam Economy."** Criminals are using technology, psychology and social media to target consumers on an unprecedented scale. Every day, thousands of fraudulent advertisements, fake websites, impersonation accounts and phishing links are created with one objective: to steal money and personal information. Fiji is not immune. As more consumers embrace online banking, digital payments and social media, scammers are adapting just as quickly. They are becoming more convincing, more organised and increasingly difficult to detect.

The recent **fake BSP loan scam circulating on Facebook** is a timely reminder that consumers must remain vigilant, and that the fight against scams requires a united national response.

When Trust Becomes a Weapon

One of the most concerning trends emerging in Fiji is the misuse of trusted brands and institutions.

Fraudsters understand that consumers are far more likely to trust a familiar logo than an unknown name. Instead of creating fake businesses from scratch, they imitate respected organisations, banks, government agencies and well-known companies to gain credibility.

The current BSP loan scam demonstrates this tactic perfectly.

Fraudulent Facebook pages are advertising **"instant BSP loans"** with promises of quick approvals, minimal documentation and immediate access to funds. These pages prominently display the BSP logo, use the bank's colours and branding, and publish professionally designed graphics that closely resemble genuine bank advertisements.

To an unsuspecting consumer, these promotions can appear completely legitimate.

Once consumers express interest, they are encouraged to communicate through Facebook Messenger or WhatsApp rather than official BSP channels. They may then be asked to provide personal information, banking details, identification documents or make upfront "processing" or "activation" payments before a loan is supposedly released. In other variations, consumers are directed to fraudulent websites designed to capture internet banking usernames, passwords

Head Office
Level 5 Vanua House
Victoria Parade GPO, Suva
Phone: 3300792/3310183
CEO: 3305864
Fax: 3300115
Email: complaints@consumersfiji.org

Lautoka/West
Suite 4 Popular Building
Vidilo Street
P.O. Box 5396, Lautoka
Phone: 6664987
Email: consumerltk@connect.com.fj

Labasa/North
Shop 2, Mudaliar Investment
Sangam Avenue Street
P.O. Box 64, Labasa
Phone: 8812559
Email: colbs@connect.com.fj

or one-time passwords (OTPs). These credentials can then be used to access victims' bank accounts.

BSP Fiji including other banks have confirmed that it **does not request passwords, PINs or OTPs through telephone calls, email, SMS or social media**, and has been actively working with authorities and online platforms to remove fraudulent content.

The New Face of Scams

Today's scammers no longer rely solely on poorly written emails or suspicious text messages. Artificial intelligence, graphic design software and social media advertising tools have made it easier than ever to create convincing scams. Criminals can now produce realistic logos, professional advertisements, fake customer testimonials and websites that closely mimic legitimate organisations.

Looking ahead, consumers can expect to see:

- AI-generated fake customer service representatives;
- Deepfake videos impersonating trusted individuals;
- Voice cloning scams using recordings from social media;
- QR code scams directing users to fake payment websites;
- Investment scams disguised as legitimate business opportunities; and
- More sophisticated phishing attacks targeting online banking customers.

Rather than hacking computer systems, many scammers simply manipulate people into voluntarily providing the information they need. This form of deception, known as social engineering, remains one of the most effective weapons in the scam economy.

Why Consumers Continue to Fall Victim?

There is a common misconception that scams only target older people or those with limited digital skills. In reality, anyone can become a victim.

Today's scammers are skilled manipulators who exploit human emotions rather than technological weaknesses. They create a false sense of urgency, excitement or fear to pressure people into making quick decisions without taking the time to verify the information.

Messages such as **"Instant loan approval," "Limited-time offer," "Your account will be suspended,"** or **"Verify your account immediately"** are carefully crafted to provoke an emotional response and encourage immediate action. Once a person acts impulsively, they are more likely to share personal information, click on malicious links or transfer money before realising they have been deceived.

Scammers also understand the power of trust. By impersonating reputable banks, government agencies or well-known organisations, they create a false sense of legitimacy that can mislead even cautious individuals.

The reality is that falling victim to a scam is not a reflection of a person's intelligence or education. Even financially savvy and digitally literate consumers can be deceived when fraudsters convincingly imitate trusted institutions and exploit moments of urgency or vulnerability. This is why staying informed, remaining cautious and always verifying unexpected requests are essential safeguards in today's increasingly sophisticated scam landscape.

A National Response is Essential

The growing scam economy cannot be addressed by consumers alone.

Banks, telecommunications providers, digital platforms, regulators, law enforcement agencies and consumer protection organisations all have a shared responsibility to reduce scam-related harm.

Financial institutions continue to strengthen fraud detection systems, monitor suspicious transactions and educate customers. The Fiji Police Force, Reserve Bank of Fiji and members of the National Anti-Scams Taskforce are working together to investigate emerging threats and disrupt criminal networks. Meanwhile, organisations such as the Consumer Council of Fiji continue to raise public awareness and assist consumers affected by deceptive practices. However, technology alone cannot eliminate scams.

How Consumers Can Protect Themselves

Consumers can significantly reduce their risk by following a few simple precautions:

- **Verify before you trust.** Always confirm loan offers, promotions or banking requests through the organisation's official website, verified social media page or customer service number.
- **Never share confidential banking information.** Banks will never ask for your Internet Banking password, PIN, CVV or OTP through Facebook, WhatsApp, SMS, email or telephone.

- **Be cautious of instant loan offers.** Legitimate financial institutions follow formal lending processes and do not guarantee immediate approval through social media.
- **Avoid clicking suspicious links.** Instead, manually type your bank's website into your browser or use the official mobile banking application.
- **Do not make upfront payments.** Genuine lenders do not require processing fees or activation charges before releasing approved loans.
- **Look for warning signs.** Poor grammar, unusually attractive offers, requests for secrecy and pressure to act quickly should immediately raise suspicion.
- **Report suspicious pages.** Reporting fraudulent Facebook pages helps prevent others from becoming victims.

Staying One Step Ahead

The scam economy is constantly evolving, and so are the tactics used by fraudsters. As technology becomes more advanced, scammers will continue to exploit new platforms, impersonate trusted organisations and develop increasingly sophisticated methods to deceive consumers. The question is no longer whether scams will become more convincing, they undoubtedly will. The real challenge is ensuring that consumers, businesses, financial institutions and regulators stay one step ahead.

While banks and authorities continue to strengthen security measures and disrupt fraudulent activities, consumer awareness remains the first and most effective line of defence. Every consumer has a role to play in protecting themselves, their families and their communities from becoming the next victim. Before responding to an unexpected message, clicking on a link, sharing personal information or transferring money, take a moment to **Stop, Think and Verify**. A few extra minutes spent confirming the legitimacy of a request could prevent the loss of your savings and personal information.

The Council urges all consumers to remain vigilant; question offers that seem too good to be true and verify all financial transactions through official channels. Suspicious websites, social media pages, phone calls and messages should be reported immediately to the relevant authorities and financial institutions to help prevent others from falling victim. The fight against scams is a shared responsibility. By working together, consumers, financial institutions, telecommunications providers, digital platforms, regulators and law enforcement agencies, we can strengthen our collective resilience against fraud and create a safer digital environment for everyone.

An informed consumer is an empowered consumer. Together, let us stay one step ahead of scammers and build a safer, smarter and more scam-resilient Fiji.