# CYBER SECURITY

# IN VANUATU

Securing Vanuatu's Digital Future

# *Cyber Security in Vanuatu –*

*Securing Vanuatu's Digital Future*

## *Introduction.*

Cybersecurity is the practice of protecting internet-connected systems of hardware, software, and data from digital threats. Its importance is global – cybercrime could reach an estimated US $10.5 trillion per year by 2025 – so for Vanuatu it is critical to build strong defenses. As Vanuatu's internet and mobile networks grow, everyone becomes exposed: for example, in November 2022 a suspected ransomware attack shut down all government systems such as parliament, police, Prime Minister's office, hospitals, Civil Registry, Customs, Finance for over 11 days, disrupting services to over 315,000 people.

This shows that even Pacific Island Nations are not immune from malicious actors. Cybersecurity helps Vanuatu protect sovereign data, personal data, maintain continuity of commerce and services and builds trust in the digital economy.

## *Introduction to Cyber Security*

Cybersecurity means defending computers, networks and data from criminals and other threats. Globally it's critical – cyber criminals can steal personal and financial data, disrupt businesses, and even threaten national security. In Vanuatu's context, expanding connectivity (internet, mobile apps, e-government) brings both opportunity and risk. For instance, after the 2022 ransomware attack, basic tasks like paying taxes or issuing licenses were delayed for weeks. **Cyber-attacks can target anyone**: you at home, government offices, schools, clinics and private businesses. Strong cybersecurity means using good practices (like strong passwords and backups) and resilient systems to prevent and mitigate these digital disasters.

DCDT

DCDT

DEPARTMENT OF COMMUNICATION
& DIGITAL TRANSFORMATION

*Empowering Connection & Shaping Tomorrow*

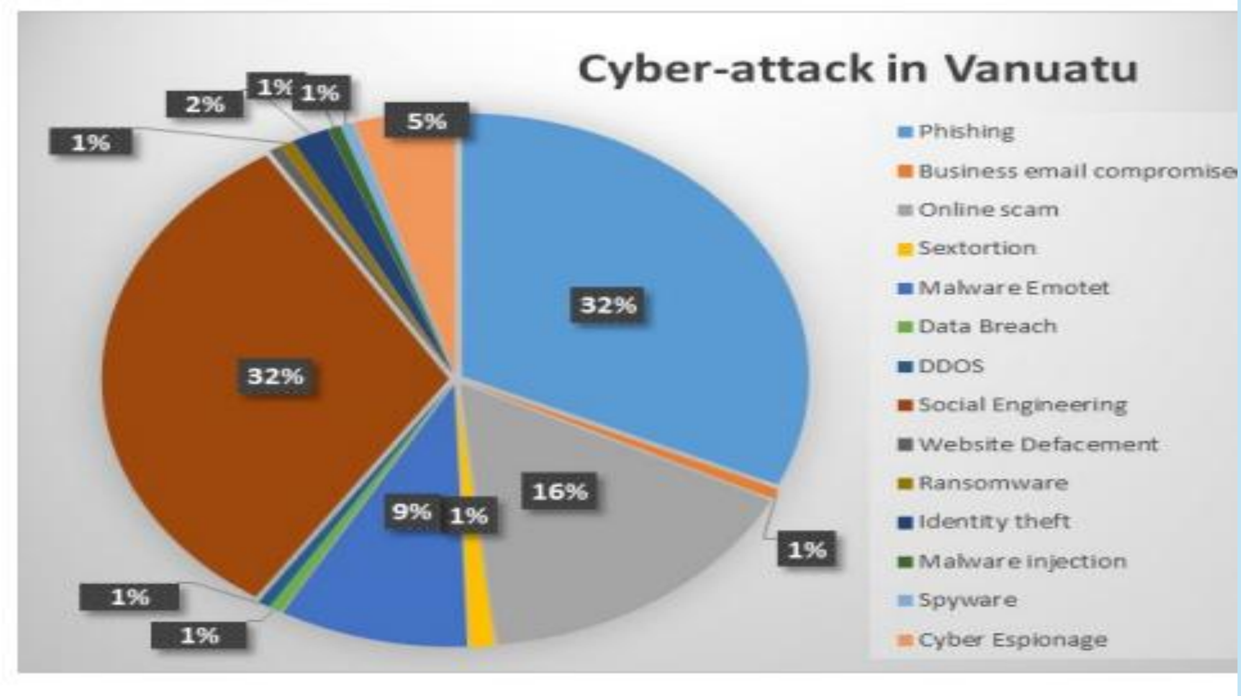
*Department responsible for Cyber Security or Leading Agency of Vanuatu Cyber Security*.

## *Cyber Threats and Risks in Vanuatu*

Common cyber threats in Vanuatu mirror global trends. These include:

- **Phishing and Scams:** Fraudulent emails or texts that trick users into revealing passwords or clicking malicious links.
- **Malware and Ransomware:** Viruses, trojans or ransomware that steal data or lock files until a ransom is paid.
- **Business Email Compromise (BEC):** Fraud where criminals spoof executives to trick businesses into transferring funds.
- **Malicious Ads and Counterfeits:** Fake social media ads or counterfeit mobile apps that install spyware.

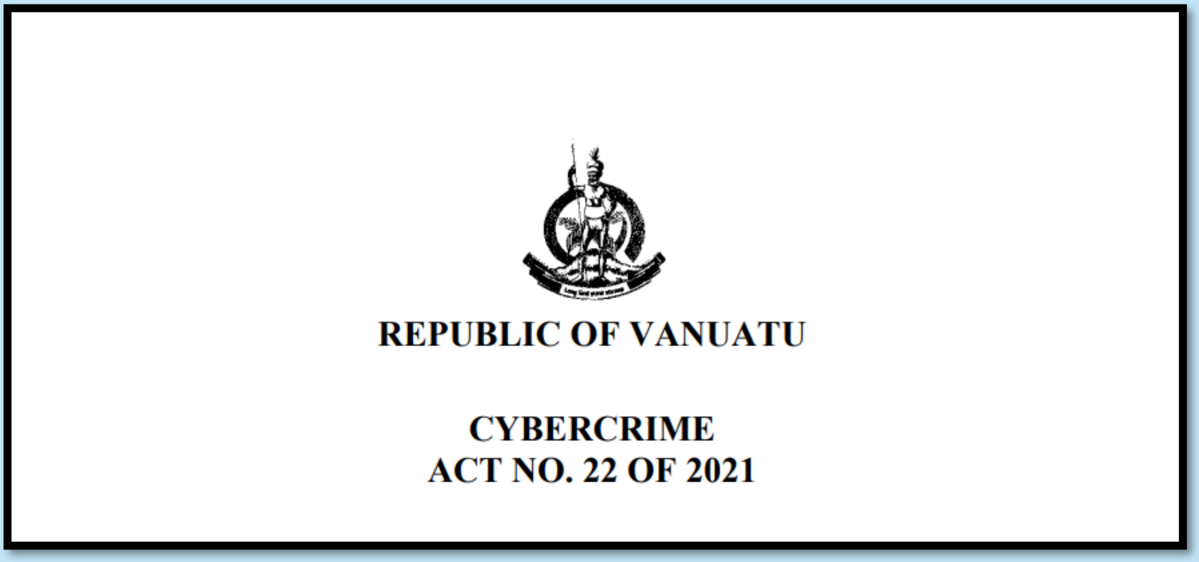
Reported cases in Vanuatu already show a rising tide of such incidents. The 2022 attack is one high-profile example. At the same time, typical vulnerabilities – weak passwords, outdated software, lack of encryption or user awareness – can amplify these risks. If users or organizations do not stay vigilant, attacks will eventuate. The threat landscape is always evolving, new forms of fraud and malware appear regularly. Keeping software updated, using security tools such as antivirus and firewalls, and educating people about phishing, can help manage these risks.



*Reported and Recorded Cyber-threats in Vanuatu*

## *Cybercrime and Law Enforcement*

Vanuatu has taken strategic steps to clamp down on cybercrime. In 2021 it enacted the **Cybercrime Act (No. 22 of 2021)** which aims at  protecting the confidentiality, integrity and availability of computer systems, programs and data. The Act highlights offences for activities such as the unauthorized access (hacking), data interference, and online fraud, aligning with international laws. It also empowers the police with new tools (e.g., data search/seizure) to investigate digital crimes.



REPUBLIC OF VANUATU

CYBERCRIME
ACT NO. 22 OF 2021

*Vanuatu Cyber Security Act*

Enforcement is in the jurisdiction of the Vanuatu Police Force (VPF) and **CERT Vanuatu** (Computer Emergency Response Team), which was set up in 2021 under the Office of the Government Chief Information Officer Now Department of communication and Digital Transformation (DCDT). CERT Vanuatu monitors attacks, issues alerts, and helps coordinate incident response. However, like many nations, law enforcement resources are limited. The VPF are still building capacity: they work with regional/international partners on serious cases and have conducted some cybercrime training. Continued investment is needed so that investigators can trace cyber criminals and prosecute them effectively. Over time, better training for officers and public reporting channels will improve the legal response to cybercrime.

*CertVu Contact Information*

## *Government Policies and Infrastructure*

Vanuatu has a National Cybersecurity Strategy to help improve and secure its digital infrastructure.

The Strategy sets six priorities:

(1) building national cyber resilience,

(2) raising public awareness of threats,

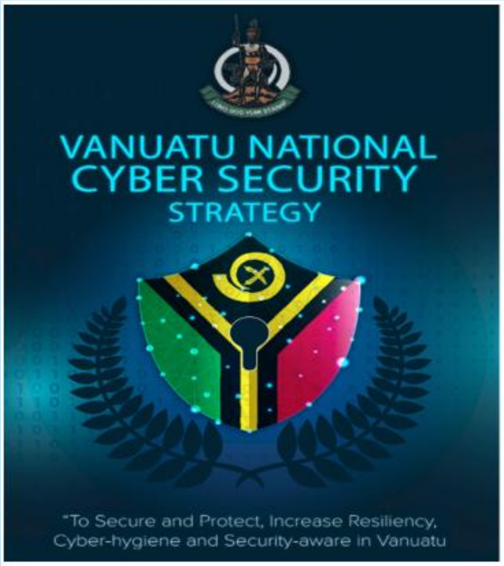
(3) developing local cybersecurity skills,

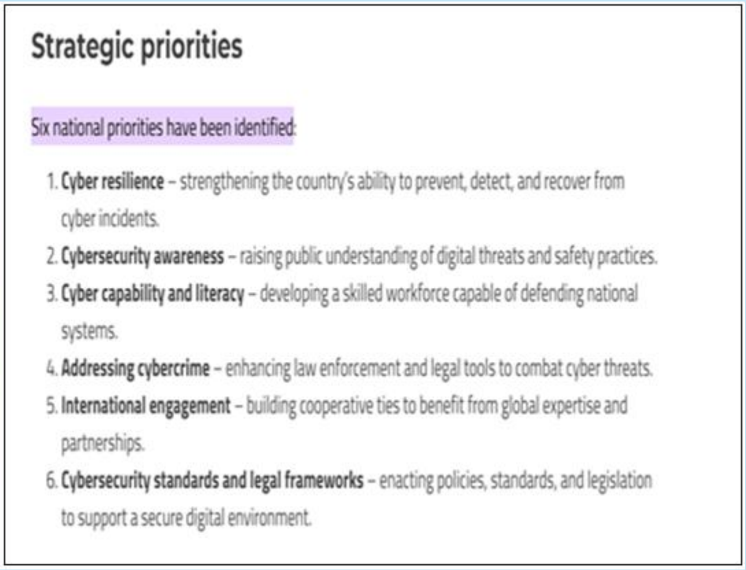
(4) strengthening laws to fight cybercrime,

(5) engaging internationally (sharing expertise), and

(6) establishing robust standards and regulations.

In practice, this means running awareness campaigns, integrating security into all government projects, and planning new agencies or frameworks as needed. For example, the strategy plans annual events (like a "Cyber Smart Pacific Month") to educate citizens and businesses on cyber hygiene and digital security.


VANUATU NATIONAL
CYBER SECURITY
STRATEGY
"To Secure and Protect, Increase Resiliency,
Cyber-hygiene and Security-aware in Vanuatu



### Strategic priorities

Six national priorities have been identified:

1. **Cyber resilience** – strengthening the country's ability to prevent, detect, and recover from cyber incidents.
2. **Cybersecurity awareness** – raising public understanding of digital threats and safety practices.
3. **Cyber capability and literacy** – developing a skilled workforce capable of defending national systems.
4. **Addressing cybercrime** – enhancing law enforcement and legal tools to combat cyber threats.
5. **International engagement** – building cooperative ties to benefit from global expertise and partnerships.
6. **Cybersecurity standards and legal frameworks** – enacting policies, standards, and legislation to support a secure digital environment.

### ***Digital infrastructure***

On the infrastructure side, Vanuatu has made good progress in upgrading its networks. Since 2014 the country's main internet link is the **ICN1 submarine fiber cable** to Fiji, providing about 20 Gbps capacity – over 200 times more bandwidth than the old satellite link. This cable significantly improved connectivity and reliability. Two additional cables (ICN2/ICN3) are planned to provide redundancies and faster speeds. Such digital infrastructure is crucial – reliable high-speed networks allow secure cloud services, data backups and quick updates across the country. In summary, the government has laid the groundwork with strategies and more resilient networks; ongoing efforts to deploy fiber cables and strengthen telecommunications will further support cybersecurity.

## *Cyber Security Education and Best Practices*

Building awareness is key. The government and partners have begun educational outreach. CERT Vanuatu and local tech organisations have run a number of ICT bootcamps and workshops in schools and communities to help sensitize the general public about best practices. The Strategy specifically calls for expanding *cyber awareness* and workforce training. For everyday users and businesses, basic security practices makes a big difference. Key recommendations include:

- **Use strong, unique passwords**. Never use the same password for multiple accounts and change passwords regularly.
- **Enable multi-factor authentication (MFA)** where available – for email, banking, social accounts, etc. This extra step (e.g. a code on your phone) greatly reduces risk.
- **Keep devices and software updated.** Regularly install updates and patches on computers, phones, routers, etc., so known vulnerabilities are fixed.
- **Back up important data.** Maintain copies of critical files (on external drives or cloud storage). If ransomware strikes, backups allow recovery without paying.
- **Be cautious with emails and links.** Don't open attachments or click links from unknown senders. Verify unexpected requests by contacting the person or company through official channels.

Businesses should train their staff on these practices and have clear IT security policies. Parents and teachers can talk to youth about digital safety (since children are increasingly online). The government's "Cyber Smart" campaigns and school programs aim to teach safe habits. Over time, a culture of security – where everyone follows good cyber hygiene – will greatly reduce vulnerabilities.

*Promote Workplace Cyber Security Awareness and Best Practices*

## *Outlook and Recommendations*

Looking ahead, cybersecurity will become even more important for Vanuatu. As more devices (phones, tablets, IoT) connect to the internet, new risks will emerge (for example, insecure IoT devices or AI-powered attacks). Regional trends suggest cyberattacks are rising sharply: one expert noted that small Pacific Island Countries face a "300% increase in cyber-attacks" without enough skilled defenders. Like its neighbors, Vanuatu must strengthen both its technology and its human resource.

Key recommendations for the future include **investing in people and policy**.

- Continue training programs to build a pool of local cyber experts and raise public awareness. Review and update laws (e.g., consider enacting a data protection law) so that legal defences keep pace with new threats.
- Ensure critical infrastructure (power, telecoms, finance, health) have robust cybersecurity measures and backup systems in place.
- Maintain and fund CERT Vanuatu and encourage private sector security initiatives.
- Keep engaging with international partners: through alliances / MOUs and information-sharing, Vanuatu can gain advanced tools and intelligence.

Vanuatu has established a solid foundation: a National Cybersecurity Strategy, a cybercrime legislation and better networks. To keep Vanuatu safe, these initiatives must be matched by **ongoing education, strong security habits (by citizens, businesses, and government), and cross-sector cooperation**. By staying vigilant and proactive, Vanuatu can protect its growing digital society and ensure a secure and resilient future.