ESSENTIAL SECURITY GUIDE

Cybersecurity Essentials for NGOs

A Practical Guide to Protecting Your Not-for-Profit Organisation from Cyber Threats in Aotearoa New Zealand and Australia

VERSION	YEAR	PUBLISHER
1.0	2025	AmplifyData.org.nz

Phishing Prevention | Password & MFA | Cloud Security | Incident Response | Data Backup | Compliance

Table of Contents

ntroduction

y Cybersecurity Matters for NGOs

Not-for-profit organisations are increasingly targeted by cybercriminals. Despite often having smaller budgets and limited IT resources, NGOs hold valuable data — donor financial information, beneficiary personal details, volunteer records, and sensitive programme data — making them attractive targets.

Why NGOs Are Targeted

Valuable Data Assets

- Donor credit card and bank details
- High-net-worth individual contact information
- Beneficiary sensitive personal data
- Grant and funding information

Limited Cybersecurity Resources

- Small or no dedicated IT staff
- Tight budgets for security tools
- Reliance on volunteers with varying tech skills
- Legacy systems and outdated software

Trust-Based Culture

- Open, collaborative work environment
- High staff turnover and volunteers
- Less formal security policies
- Tendency to trust communications

Wide Attack Surface

- Multiple locations and remote workers
- Shared devices and BYOD policies
- Cloud services and online donations
- Public-facing websites and email

The Cost of a Cyber Attack

IMPACT AREA	CONSEQUENCES
Financial	Direct theft, fraud, ransom payments, recovery costs, legal fees
Reputational	Loss of donor trust, media coverage, reduced giving, partner concerns
Operational	Service disruption, staff time diverted, programme delays
Legal/Regulatory	Privacy breach notifications, fines, investigations
Beneficiaries	Exposure of vulnerable populations' data, service interruption

Cyber Incident Statistics (2023-2024)

67%	31%	23%	72%
PHISHING ATTACKS	BUSINESS EMAIL COMPROMISE	RANSOMWARE	ORGANISATIONS UNPREPARED

AVERAGE COST OF A CYBER INCIDENT

$45,000 – $125,000 NZD with an average recovery time of **2–6 weeks**.

Executive Summary for Boards

KEY MESSAGES

1. **Cyber attacks on NGOs are increasing** — 1 in 4 Australian charities and 1 in 5 NZ NGOs experienced a cyber incident in the past year
2. **Small organisations are not immune** — 43% of attacks target organisations with under 50 staff
3. **Most attacks are preventable** — 90% of successful attacks exploit human error or basic security gaps
4. **Compliance is mandatory** — Privacy Act (NZ) and Privacy Act 1988 (AU) require "reasonable security measures"
5. **Investment is modest** — basic protections can be implemented with minimal budget

nderstanding the Threat Landscape

mmon cyber threats facing not-for-profit organisations

Common Cyber Threats

External Threats

- ☐ Phishing emails
- ☐ Ransomware
- ☐ Business email compromise
- ☐ Website attacks
- ☐ Social engineering
- ☐ Credential stuffing

Internal Threats

- ☐ Accidental data exposure
- ☐ Lost/stolen devices
- ☐ Departing staff access
- ☐ Shadow IT
- ☐ Poor password practices
- ☐ Untrained volunteers

Environmental

- ☐ Natural disasters
- ☐ Power outages
- ☐ Internet failures
- ☐ Hardware failures

Systemic

- ☐ Outdated software
- ☐ Unpatched systems
- ☐ Lack of backups
- ☐ No incident plan

Types of Phishing

TYPE	DESCRIPTION	NGO EXAMPLE
Mass Phishing	Generic emails sent to thousands	"Your Microsoft account needs verification"
Spear Phishing	Targeted emails using personal info	"Hi Sarah, please review this grant proposal"
Whaling	Targeting executives	Email appearing from Board Chair to CEO
Business Email Compromise	Impersonating trusted parties	Fake invoice from regular supplier
Smishing	SMS-based phishing	Text about failed donation payment
Vishing	Phone-based scams	Call claiming to be from IT support

Ransomware Attack Lifecycle

1
Initial Access
Phishing email, malicious download, or compromised credentials

→

2
Lateral Movement
Explore network, steal credentials, identify data

→

3
Encryption
Lock files, delete backups, disable recovery

→

4
Extortion
Demand payment, threaten data release

$50K–$500K
AVERAGE RANSOM (NZD)

21 days
AVERAGE DOWNTIME

65%
RECOVERY WITHOUT PAYING (GOOD BACKUPS)

Business Email Compromise Scenarios

CEO Fraud
Email appears from CEO to Finance Manager requesting an urgent wire transfer for a "time-sensitive grant matching opportunity."
Loss: $15,000 – $150,000

Supplier Impersonation
Email appears from regular vendor claiming bank details have changed and requesting updated payment information.
Loss: $5,000 – $50,000

Grant Fraud
Email appears from funder requesting bank details for an "urgent grant disbursement."
Loss: Grant amount + reputation damage

Donation Diversion
Attacker gains email access and contacts major donors requesting donations to a fraudulent bank account.
Loss: Varies + donor relationship damage

hishing & Social Engineering

ognising, preventing, and responding to phishing attacks

Recognising Phishing Emails

PHISHING RED FLAGS CHECKLIST

- ☐ Sender email address looks suspicious (hover to see actual address)
- ☐ Hover over links BEFORE clicking — does URL match expected destination?
- ☐ Generic greetings ("Dear Customer" instead of your name)
- ☐ Spelling and grammar errors
- ☐ Urgency or threat language
- ☐ Requests for personal information
- ☐ Unexpected attachments
- ☐ "Too good to be true" offers
- ☐ Mismatched branding or formatting
- ☐ Requests to bypass normal procedures

Real-World NGO Phishing Examples

Fake Funder Email

From: grants@community-foundation.org.nz.**secure-portal.com**

"Congratulations! Your application has been shortlisted. Confirm your bank details through our secure portal within 48 hours."

Red flags: Domain is "secure-portal.com" not the real foundation; urgency; request for bank details via link.

CEO Impersonation

From: john.smith@you**m**go.org.nz (note misspelling)

"I'm in a board meeting and can't talk but need you to urgently process a payment of $12,500."

Red flags: Misspelled domain; claims unavailability; urgent new payment; pressure to bypass approvals.

Suspicious Email Response Protocol

1
Don't Click
Never click links or open attachments

→

2
Verify
Call sender on known number, check real email

→

3
Report
Forward to IT support, manager, or CERT NZ / ACSC

→

4
Delete
Remove the email from your inbox

Social Engineering Verification Procedures

REQUEST TYPE	VERIFICATION METHOD
Payment change request	Call supplier on known number (not from email)
Urgent fund transfer	Two-person approval, verbal confirmation
Password reset request	In-person or video call verification
IT support request	Verify caller identity, call back on known number
Data access request	Written approval from data owner

assword Security & MFA

ong passwords and multi-factor authentication

Creating Strong Passwords

RECOMMENDED REQUIREMENTS

- **Minimum Length:** 16+ characters (passphrases best)
- **Complexity:** Mix of words, numbers, symbols
- **Uniqueness:** Different password for every account
- **Rotation:** Only when compromised (not time-based)

GOOD VS BAD EXAMPLES

Good: correct-horse-battery-staple

Good: Kiwi$Running%Through@Forest42

Bad: password123

Bad: CharityNZ2024

Password Manager Comparison

FEATURE	BITWARDEN	1PASSWORD	LASTPASS	KEEPER
Free Tier	Yes (full featured)	No	Limited	No
Nonprofit Discount	Yes (free for small)	50% off	50% off	Yes
Team Features	Yes	Yes	Yes	Yes
Ease of Use	Good	Excellent	Good	Good
Recommended For	Budget-conscious	Ease of use	Established teams	Enterprise

Multi-Factor Authentication (MFA)

MFA requires two or more verification methods, dramatically reducing account compromise risk.

Strongest	**Hardware keys**	(YubiKey, Titan) — physical device required, phishing resistant. Best for high-risk accounts.

Strong	**Authenticator apps** (Microsoft, Google, Authy) — time-based codes, harder to intercept. Recommended for most accounts.
Moderate	**SMS/Text message codes** — better than nothing but can be intercepted via SIM swap. Use only if no other option.
Weak	**Email codes**— if email is compromised, MFA is bypassed. Avoid for important accounts.

MFA Implementation Priority

PRIORITY	ACCOUNT TYPE	RECOMMENDED MFA
Critical	Admin accounts (M365, Google Workspace)	Hardware key or authenticator app
Critical	Financial systems (banking, accounting)	Hardware key or authenticator app
Critical	CRM with donor data	Authenticator app
High	Email accounts	Authenticator app
High	Cloud storage	Authenticator app
Medium	Social media accounts	Authenticator app
Medium	Website admin	Authenticator app

mail Security

uring your email platform and establishing safe practices

Email Security Layers

01

Platform Security

- Enable MFA for all accounts
- Use strong, unique passwords
- Configure admin account protection
- Enable audit logging

02

Filtering & Protection

- Enable spam filtering
- Configure phishing protection
- Block dangerous file types
- Enable link scanning

03

Policies & Settings

- Disable auto-forwarding to external addresses
- Configure external email warnings
- Set up DMARC, DKIM, SPF
- Enable mailbox auditing

04

User Practices

- Verify unexpected requests
- Don't click suspicious links
- Report phishing attempts
- Think before sending sensitive data

Email Authentication (SPF, DKIM, DMARC)

SPF

Sender Policy Framework — lists authorised servers that can send email for your domain. Prevents spoofing from unauthorised servers.

DKIM

DomainKeys Identified Mail — adds digital signature to outgoing emails. Proves email wasn't modified in transit.

DMARC

Domain-based Message Authentication — tells receiving servers what to do with failed SPF/DKIM. Ultimate goal: policy = reject.

Secure Email Practices

DO	DON'T
Verify unexpected requests via phone	Click links in unexpected emails
Check sender email addresses carefully	Open attachments from unknown senders
Use encrypted file sharing for sensitive data	Send passwords or bank details via email
Report suspicious emails immediately	Reply to suspected phishing
Encrypt emails containing personal information	Auto-forward to personal accounts

evice Security

nputer and mobile device protection essentials

Computer Security Essentials

Operating System

- Use supported OS (Windows 10/11, macOS 12+)
- Enable automatic updates
- Configure automatic restart for updates

Security Software

- Enable built-in protection (Defender, macOS)
- Configure automatic scans
- Enable real-time protection

Encryption

- Enable full disk encryption (BitLocker / FileVault)
- Verify encryption is active

Access Controls

- Require password/PIN to unlock
- Auto-lock (5 minutes max)
- Disable guest accounts
- Use standard (non-admin) accounts daily

Endpoint Protection Solutions

SOLUTION	COST	BEST FOR	FEATURES
Windows Defender	Free (built-in)	Basic protection	Antivirus, firewall, ransomware protection
Microsoft Defender for Business	~$3/user/month	M365 users	Advanced protection, threat detection
Malwarebytes	Free/Premium	Additional scanning	Malware removal, real-time (premium)
CrowdStrike Falcon Go	~$5/user/month	Growing teams	Cloud-based, behavioural detection

Update Priority

Critical	**Security updates**— apply within 24–48 hours
High	**Operating system updates**— apply within 1 week
Medium	**Application updates**— apply within 2 weeks
Low	**Feature updates**— plan and test first

etwork & Wi-Fi Security

ce network protection and Wi-Fi best practices

Wi-Fi Security Requirements

SETTING	REQUIREMENT	WHY
Encryption	WPA3 (or WPA2 minimum)	WEP and open networks easily compromised
Password	Strong, unique passphrase	Prevents unauthorised access
SSID	Don't include organisation name	Reduces targeting
Guest Network	Separate network for visitors	Protects internal resources
Router Admin	Change default password	Default credentials publicly known
Firmware	Keep updated	Patches security vulnerabilities

VPN Usage Guide

USE VPN WHEN

- Working from home
- Using public Wi-Fi (cafes, airports, hotels)
- Accessing sensitive organisational systems
- Working from co-working spaces
- Travelling internationally

VPN OPTIONS FOR NGOS

- **Microsoft 365 / Azure VPN:** Included with some licences
- **Cloudflare WARP:** Free basic tier
- **TechSoup donated solutions**
- **Enterprise VPN** for larger organisations

ata Backup & Recovery

kup strategies, solutions, and disaster recovery

The 3-2-1 Backup Rule

3

Copies of Data

Original (working copy) + Backup #1 (on-site or cloud) + Backup #2 (off-site)

2

Different Media Types

Cloud storage + external drive OR different cloud provider

1

Off-Site Copy

Cloud backup OR physical off-site location (protects against fire, flood, theft)

Backup Priority Matrix

PRIORITY	DATA TYPE	EXAMPLES	FREQUENCY
Critical	Financial records	Xero exports, bank statements	Daily
Critical	Donor database	CRM exports, donation records	Daily
Critical	Legal documents	Contracts, policies, minutes	Daily
High	Client/beneficiary records	Case files, programme data	Daily
Medium	Documents and files	Word, Excel, proposals	Daily
Medium	Website	Database, content, theme	Weekly

Backup Testing Schedule

Monthly Tests

- Verify backup jobs completed
- Check logs for errors
- Confirm backup size is growing
- Restore one random file

Quarterly Tests

- Full restore to separate location
- Test critical systems restore
- Document recovery time (RTO)
- Verify data integrity

Annual Tests

- Full disaster recovery simulation
- Test restore to different hardware
- Review and update procedures
- Update all documentation

loud Security

uring Microsoft 365 and Google Workspace

Microsoft 365 Security Essentials

Identity & Access

- Enable MFA for all users
- Block legacy authentication
- Limit Global Admin accounts (2–4 max)
- Configure Conditional Access

Data Protection

- Enable sensitivity labels
- Configure DLP policies
- Disable anonymous sharing links
- Set sharing defaults to "specific people"

Email Security

- Configure anti-phishing policies
- Enable Safe Links & Safe Attachments
- Block auto-forwarding externally
- Configure SPF, DKIM, DMARC

Monitoring

- Review Security Score weekly
- Set up alert policies
- Review sign-in logs monthly
- Enable Cloud App Security alerts

Cloud File Sharing Security

SHARING METHOD	USE WHEN	SECURITY CONSIDERATIONS
Specific people	Sharing with known individuals	Most secure, tracks access
Anyone in org	Internal sharing	Good for collaboration
Anyone with link	AVOID for sensitive data	No access control, can be shared
Expiring links	Temporary external sharing	Better than permanent links
Password-protected	Extra layer for sensitive files	Adds barrier, not foolproof

emote Work Security

uring home offices, public Wi-Fi, and BYOD

Home Office Security Checklist

Home Network

- Change router admin password from default
- Update router firmware
- Use WPA3/WPA2 encryption
- Use strong Wi-Fi password
- Disable remote router management

Workspace Security

- Position screen away from windows
- Lock device when away
- Use privacy screen in shared spaces
- Store documents securely
- Shred physical documents with PII

Device Security

- Use organisation-provided device
- Enable full disk encryption
- Keep software updated
- Lock when stepping away
- Don't share with family members

Data Handling

- Avoid printing sensitive documents
- Don't save to personal cloud
- Use approved file storage
- Clear browser data regularly
- Log out when done

Public Wi-Fi Safety

PROTECTION MEASURES FOR PUBLIC WI-FI

1. Use mobile data instead when possible
2. Use VPN for all connections
3. Verify network name with staff
4. Only access HTTPS websites
5. Avoid accessing banking or sensitive systems
6. Disable auto-connect to Wi-Fi
7. Turn off file sharing
8. Use mobile hotspot from your phone

endor & Third-Party Risk

essing and managing vendor security

Vendor Security Tiers

TIER	DATA ACCESS	ASSESSMENT LEVEL	EXAMPLES
Tier 1 (Critical)	Sensitive data, system access	Full security assessment, annual review	CRM, accounting, email
Tier 2 (High)	Some personal data	Security questionnaire, bi-annual review	Marketing platforms, event tools
Tier 3 (Medium)	Limited data access	Basic questionnaire	Website hosting, design tools
Tier 4 (Low)	No data access	Standard terms review	Office supplies, utilities

Secure Data Sharing Process

1
Determine Necessity
Minimum data needed? Can we anonymise?

→

2
Verify Security
Complete vendor assessment

→

3
Establish Agreements
DPA, NDA, use limitations

→

4
Secure Transfer
Encrypted methods, no bulk email

→

5
Track & Exit
Log sharing, revoke on exit

ncident Response Planning

paring for and responding to security incidents

Incident Response Team Roles

ROLE	RESPONSIBILITIES	WHO (TYPICAL)
Incident Lead	Coordinate response, make decisions	CEO or Operations Manager
Technical Lead	Investigate, contain, remediate	IT person, MSP, or consultant
Communications	Internal/external messaging	CEO or Comms Manager
Legal/Compliance	Privacy obligations, legal advice	Board member or external counsel
Documentation	Record actions, timeline, evidence	Any team member

Incident Response Phases

1 **Detect** — Assess & classify severity → 2 **Contain** — Isolate systems, preserve evidence → 3 **Eradicate** — Remove threat, patch vulnerabilities → 4 **Recover** — Restore from backups, monitor → 5 **Review** — Lessons learned, update controls

Incident Severity Classification

Critical	**Respond immediately**	— active ransomware, confirmed data breach with PII, complete outage, ongoing theft of funds
High	**Respond within 1–4 hours**	— suspected data breach, BEC attempted, malware on multiple systems
Medium	**Respond within 24 hours**	— phishing campaign targeting staff, single device infection, suspicious activity
Low	**Respond within 72 hours**	— minor policy violations, spam increase, isolated suspicious activity

Quick Reference Card

WHEN AN INCIDENT OCCURS

1. **Don't panic — document:** What happened? When? Who discovered it? What systems/data affected?
2. **Alert the Incident Lead** immediately
3. **Contain (if safe):** Disconnect affected device from network; DON'T turn off (preserve evidence); DON'T try to fix yourself
4. **Document everything:** Take screenshots; note times and actions; save suspicious emails

External Contacts: CERT NZ: 0800 CERT NZ (cert.govt.nz) | ACSC (AU): 1300 CYBER1 (cyber.gov.au)

Breach Notification Requirements

NEW ZEALAND (PRIVACY ACT 2020)

- **When:** Privacy breach causing serious harm
- **Notify:** Affected individuals + Privacy Commissioner
- **Timeframe:** "As soon as practicable"
- **Report:** notifyme.privacy.org.nz

AUSTRALIA (PRIVACY ACT 1988)

- **When:** Eligible data breach likely to cause serious harm
- **Notify:** Affected individuals + OAIC
- **Timeframe:** Within 30 days of becoming aware
- **Report:** oaic.gov.au

taff Training & Awareness

ding a security culture across your organisation

Annual Security Training Programme

Onboarding (New Staff)

- Security policy overview
- Password and MFA setup
- Phishing awareness basics
- Device security requirements
- Incident reporting process
- Sign acceptable use policy

Monthly (All Staff)

- Phishing simulation (1–2 per month)
- Security tip email or message
- Share relevant sector news
- Quick quiz or awareness prompt

Quarterly (All Staff)

- 15–30 minute training module
- Q1: Phishing & social engineering
- Q2: Password security & MFA
- Q3: Data protection & privacy
- Q4: Physical security & travel

Annual (All Staff)

- Comprehensive refresher training
- Policy acknowledgment
- Update emergency contacts
- Review of year's incidents & learnings

Free & Low-Cost Training Resources

RESOURCE	TYPE	COST	BEST FOR
CERT NZ Resources	Guides, posters, videos	Free	NZ-specific awareness
ACSC Resources	Guides, fact sheets	Free	AU-specific guidance
KnowBe4 Free Tools	Phishing tests, training	Free tier	Basic simulation
Google Security Checkup	Self-service tool	Free	Google Workspace users
Microsoft Security Webinars	Training videos	Free	M365 users

ompliance & Regulatory Requirements

acy Act obligations for NZ and Australian NGOs

NZ Privacy Act 2020

INFORMATION PRIVACY PRINCIPLE 5 (STORAGE & SECURITY)

"An agency must ensure that personal information is protected by reasonable security safeguards against loss, unauthorised access, use, modification, disclosure, or other misuse."

What "reasonable" means: Depends on size and resources of organisation, sensitivity of information, risk of harm, current technology, and cost of measures.

Penalties: Up to $10,000 per interference with privacy, plus complaints, investigations, and civil liability.

Australian Privacy Act 1988

AUSTRALIAN PRIVACY PRINCIPLE 11 (SECURITY)

"An APP entity must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure."

Notifiable Data Breaches Scheme: Report to OAIC within 30 days. Penalties up to $2.5 million for organisations.

Essential Security Policies

01

Acceptable Use Policy

How staff/volunteers may use technology, prohibited activities, consequences

02

Password & Access Policy

Password requirements, MFA, access provisioning and removal

03

Data Classification

Classification levels, handling requirements, encryption, retention

04

Incident Response Policy

Incident definition, response procedures, roles, breach notification

05

Backup & Recovery Policy

Backup requirements, frequency, retention, testing, recovery

06

Remote Work / BYOD Policy

Device requirements, security controls, data handling, reporting

ecurity on a Budget

e and low-cost security tools and strategies

Security Investment Priorities

Tier 1	**Do Immediately (Free/$0–$500/yr)**	— MFA, password manager, auto-updates, cloud security settings, backup, basic training
Tier 2	**Near-Term ($500–$2K/yr)**	— phishing simulation, third-party backup, security policies, incident response plan
Tier 3	**Medium-Term ($2K–$10K/yr)**	— EDR, advanced email security, training programme, vulnerability assessments
Tier 4	**Long-Term ($10K+/yr)**	— security operations monitoring, advanced threat detection, cyber insurance, dedicated resource

Nonprofit Technology Discounts

PROVIDER	DISCOUNT	HOW TO ACCESS
Microsoft 365 Business Premium	Free for eligible nonprofits	TechSoup or Microsoft Nonprofits
Google Workspace	Free for eligible nonprofits	Google for Nonprofits
1Password	50% off	1password.com/nonprofits
LastPass	50% off	LastPass Nonprofit programme
KnowBe4	Nonprofit pricing	Contact KnowBe4
Cisco Umbrella	Nonprofit pricing	TechSoup

nplementation Checklists

essment tools, checklists, and implementation plan

Quick Security Assessment

Identity & Access

- ☐ MFA enabled for all staff accounts
- ☐ Password manager used organisation-wide
- ☐ Unique passwords for all accounts
- ☐ Access removed promptly when staff leave
- ☐ Admin accounts limited and protected

Device Security

- ☐ All devices on supported OS versions
- ☐ Automatic updates enabled
- ☐ Full disk encryption enabled
- ☐ Screen lock required
- ☐ Antivirus/endpoint protection active

Email Security

- ☐ Phishing protection enabled
- ☐ External email warnings configured
- ☐ Staff trained on phishing awareness
- ☐ SPF/DKIM/DMARC configured
- ☐ Auto-forwarding to external disabled

Preparedness

- ☐ Incident response plan documented
- ☐ Staff know how to report incidents
- ☐ Key contacts list current
- ☐ Insurance coverage reviewed
- ☐ Breach notification process defined

SCORING GUIDE

Rate each item: Done (2 points) | Partial (1 point) | Not Done (0 points)

20–24: Good security posture — maintain and improve | **14–19:** Moderate — address gaps promptly | **8–13:** Significant gaps | **0–7:** Critical — immediate action needed

esources & Further Reading

ditional guides, tools, and support contacts

Key Contacts

NEW ZEALAND

- **CERT NZ:** 0800 CERT NZ | cert.govt.nz
- **NZ Privacy Commissioner:** privacy.org.nz
- **NetSafe NZ:** netsafe.org.nz
- **TechSoup NZ:** techsoup.net.nz

AUSTRALIA

- **ACSC:** 1300 CYBER1 | cyber.gov.au
- **OAIC:** oaic.gov.au
- **ACNC:** acnc.gov.au
- **Connecting Up:** connectingup.org

AmplifyData.org.nz
Contact@AmplifyData.org.nz

Cybersecurity Essentials for NGOs — Version 1.0 — 2025