

Participant Handout

Protecting Trust in a Digital World: Practical Approaches for Cyber-Security

Endow Manitoba Community Foundation Conference 2026 · Saturday, April 25, 2026 · 10:30–11:45 a.m. · Lancaster Room

The 6 Threats That Matter Most

Threat	What it is	Risk
Phishing	Fake emails tricking staff into revealing passwords or clicking malware links	High
Business Email Compromise	Impersonating executives/grantees to redirect payments	High
Ransomware	Encrypting files and demanding payment to restore access	High
Social engineering	Manipulating staff by phone, text, or in-person	Medium
Credential theft	Exploiting weak/reused passwords to access systems	Medium
Vendor / third-party risk	Security gaps in donation platforms, software, or contracted services	Medium

Recognizing a Phishing Email — Teach Your Team

Watch for these warning signs before clicking any link or opening any attachment:

- **Urgency or threats** — "Act now or your account will be closed"
- **Mismatched sender address** — display name looks right but the actual email domain doesn't match
- **Unexpected requests** — asking you to verify credentials, approve a payment, or open an attachment
- **Unfamiliar links** — hover over links before clicking to see the real destination URL
- **Unusual tone or language** — even if it looks like it's from a colleague

When in doubt: pick up the phone and call using a number you already have.

The BEC Rule — Post This at Every Finance Desk

Any request to change a bank account number, redirect a payment, or authorize an urgent wire transfer must be verified by phone — on a number you already have on file — before any action is taken. No exceptions.

This single practice stops 100% of business email compromise attacks.

Your Non-Negotiable Security Essentials

Technical controls (priority order):

1. **Multi-factor authentication (MFA)** on all accounts — start with email, then banking, then donor systems
2. **Password manager** — Bitwarden is free and open-source

3. **Automatic software updates** enabled on all devices
4. **Endpoint protection** (antivirus/anti-malware) on all staff computers
5. **Email spam and phishing filtering** — built into Microsoft 365 and Google Workspace
6. **3-2-1 Backups** — 3 copies, 2 different media types, 1 offsite or in the cloud

Access management:

- Give staff access to only what they need for their role (least privilege)
- Revoke ALL access on a person's last day — use a formal offboarding checklist
- Annual review of who can access what systems
- Two-person authorization for large financial transactions

MFA: The Single Highest-Impact Action You Can Take

Microsoft research: MFA blocks 99.9% of automated account compromise attacks.

Method	Level	Notes
SMS text codes	OK	Better than nothing; vulnerable to SIM swapping
Authenticator app (MS/Google)	Recommended	Free, strong, easy to set up
Hardware key / Passkey	Best	Fully phishing-resistant

Where to enable MFA first: Email → Banking → Donor database → Cloud storage → Social media

Incident Response: Know Before You Need It

Before an incident:

- Written response plan, tested backups, cyber insurance, legal counsel identified
- Staff know who to call — build a contact list now

During an incident:

- Isolate affected devices immediately (unplug from network)
- Do NOT pay ransom without consulting a professional IR firm
- Preserve evidence — do not wipe systems
- Notify your IT support / MSSP, ED, and board chair immediately

After an incident:

- PIPEDA breach notification required if significant harm risk (within 72 hours)
- Notify affected donors and partners
- Restore from verified clean backups
- Conduct a post-incident review and update policies

Report Canadian cybercrime to: Canadian Centre for Cyber Security (cyber.gc.ca) and your local RCMP.

Free & Low-Cost Tools for Nonprofits

Tool	What it does	Cost
Microsoft 365 for Nonprofits	Email, Teams, Defender, MFA — the full suite	Free/donated via TechSoup
Google Workspace Nonprofits	Gmail, Drive, built-in security controls	Free
Bitwarden	Password manager — open-source, trusted	Free
Have I Been Pwned	Check if your email was in a known breach	Free
CIRA D-Zone DNS Firewall	Canadian DNS-based protection for nonprofits	Low cost

Canadian resources:

- **cyber.gc.ca** — Canadian Centre for Cyber Security: free guides, self-assessment, incident reporting
- **TechSoup Canada** (techsoupcanada.ca) — discounted and donated software for registered nonprofits
- **CIRA** (cira.ca) — Canadian Internet Registration Authority, nonprofit cybersecurity tools
- **GetCyberSafe.gc.ca** — Government of Canada digital safety awareness resources
- **Imagine Canada** (imaginecanada.ca) — sector resources for Canadian charities

Your 90-Day Action Plan

Days 1–30: Quick Wins

- Enable MFA on all staff email accounts
- Deploy a password manager (start with Bitwarden — it's free)
- Go to haveibeenpwned.com — check your work email address
- Test your backup: actually restore a file to confirm it works
- Create a "who do we call?" incident contact list

Days 30–60: Build Foundations

- Run a phishing awareness session with all staff
- Review and update access permissions for all staff and volunteers
- Establish a written payment verification process
- Apply for Microsoft 365 Nonprofit or Google Workspace Nonprofit (via TechSoup Canada)
- Get at least one cyber insurance quote

Days 60–90: Sustain and Improve

- Write (or update) a basic written incident response plan
- Present a security status update to your board
- Review security practices of your key vendors and donation platform
- Set a recurring annual security review date on your calendar
- Share one thing you've learned with a peer foundation

Notes

My Commitment

One action I will complete before May 25, 2026:

I told this to: _____ (table neighbour — accountability partner)

Reminder I will set on my calendar:

For questions after the conference, connect through the Endow Manitoba network or visit cyber.gc.ca for free Canadian resources.
Session presented at Endow Manitoba Community Foundation Conference 2026 · The Winnipeg Foundation · wpgfdn.org