COMMUNITY FOUNDATION CONFERENCE

Endow Manitoba

Learn. Lead. Legacy.

APRIL 24 • 26, 2026

Protecting Trust in a Digital World

Finance & Administration

Saturday, April 25, 2026 | 10:30–11:45 a.m. | Lancaster Room

Your Presenter

Sean Lynch

IT / Cybersecurity Professional

United Way Winnipeg

Welcome & Session Overview

Protecting Trust in a Digital World

What we will cover:

- The threat landscape — what your foundation is up against
- Real-world case studies from organizations like yours
- Practical, affordable defences you can implement now
- Peer discussion — share and learn from each other
- A personal 90-day action plan

What you will leave with:

- Concrete steps to protect your foundation — no large IT budget required
- One specific commitment to act on before May 25

Please ask questions throughout — this is a conversation, not a lecture.

Why Your Foundation Is a Target

64% of nonprofits have experienced a cyber incident

$164,000 average cost of a breach for a small nonprofit

9 months average time to detect a breach

Why attackers target community foundations:

- Donor data — names, addresses, giving history, and financial information
- Regular large transactions: grants, donations, endowment distributions
- High community trust makes impersonation easy and effective
- Limited IT security resources relative to the value you manage
- Volunteers on unmanaged personal devices with no security controls

The Threat Landscape

HIGH RISK

- Phishing & email fraud — fake emails tricking staff into revealing credentials or clicking malware links
- Business Email Compromise (BEC) — impersonating executives to redirect grant payments or wire transfers
- Ransomware — encrypting all your data and demanding payment, can halt operations for weeks

MEDIUM RISK

- Social engineering — manipulating staff by phone, text, or in-person to extract access or information
- Credential theft — weak or reused passwords exploited to access donor databases and financial systems
- Third-party/vendor risk — security gaps in donation platforms, software vendors, or contracted IT services

Good news: these threats are largely preventable with consistent, affordable practices.

Phishing: The Most Common Attack Vector

How it works:

- Attacker sends a convincing email from a trusted-looking source
- Link leads to a fake login page — credentials are harvested instantly
- Or attachment silently installs malware on your system
- Spear phishing = personalized attacks targeting specific named staff

Red flags to teach your team:

- Urgency — “Act now or your account will be suspended”
- Mismatched sender domain (e.g. support@rbc-secure.net — not rbc.com)
- Unexpected requests to verify credentials or payment information
- Suspicious attachments: .exe, .zip files, or macro-enabled Office documents

Defence: Security awareness training + email filtering + MFA = over 90% reduction in success

Business Email Compromise (BEC)

$2.9 BILLION+ lost globally each year to BEC (FBI IC3)

How it works:

- Executive email is compromised or impersonated via display name spoofing
- Urgent request for wire transfer or gift card purchase
- Or: grant/vendor payment redirected to a fraudulent bank account
- Funds are typically unrecoverable once transferred

Foundation-specific risks:

- Grant disbursements — “Please update our banking details before next payment”
- Board members impersonated to approve urgent financial requests
- Donation redirect fraud — fake versions of your donation page

KEY DEFENCE: Verify ALL payment changes by phone — on a known number. Never reply to the requesting email. Two-person authorization for all large transfers.

Ransomware

The attack chain:

1. **Entry:** Phishing email, RDP exploit, or stolen credentials
2. **Reconnaissance:** Attacker moves silently through your network for weeks
3. **Exfiltration:** Donor and financial data is copied before encryption
4. **Encryption:** All files locked — ransom note appears on every screen
5. **Extortion:** Pay or your donor data gets released publicly

$50K–$250K CAD average ransom demand for small organizations (without backups)

Best defences:

- 3-2-1 backup rule: 3 copies, 2 different media types, 1 offsite or cloud
- Patch and update all software promptly — most ransomware exploits known vulnerabilities
- Endpoint detection & response (EDR) tools + cyber insurance

Social Engineering: Hacking Humans

Most attacks succeed not by breaking technology — but by manipulating people.

Vishing (voice phishing):

- Calls impersonating IT support, CRA, or your bank requesting credentials or urgent gift card purchases

Pretexting:

- Fabricated story — “I’m your new IT vendor, I need your login to complete the system upgrade”

Tailgating & physical threats:

- Following authorized staff into secure areas; USB drives left in parking lots as bait

AI deepfakes (emerging threat):

- AI-cloned voice or video of your ED or board chair requesting urgent financial action

KEY DEFENCE: Build a culture where verifying any unusual request is expected and

Case Study: Your Real-World Story

[PRESENTER — replace this slide with your own story]

Attendees expect “real world experiences” — your personal story is the most powerful part of this session.

Suggested structure:

1. **Context:** Organization type and situation (anonymize details as needed)
2. **The attack:** What happened? How did the attacker gain access?
3. **The impact:** Financial, operational, and reputational cost
4. **The response:** What did you do? What worked and what didn’t?
5. **The lesson:** What can everyone in this room apply today?

Aim for 5–7 minutes. Be specific and honest — real stories teach far more than statistics.

Real-World Examples

CASE 1 — BEC Wire Fraud — $500,000 loss

- Finance staff received a convincing email appearing to be from the Executive Director requesting an urgent grant payment to a new bank account. No phone verification was done. Funds were unrecovered.

CASE 2 — Ransomware Attack — 3 weeks offline

- A single clicked phishing email encrypted donor records, grant databases, and all financial systems. The foundation paid the ransom and spent months rebuilding donor and community trust.

CASE 3 — Donor Database Breach — 4,000 donors affected

- A former staff member retained active credentials after departure. 4,000 donor records were exfiltrated. PIPEDA breach notification was required. Significant reputational damage resulted.

Common thread: in each case, one simple practice would have stopped it.

The Essentials

Technical controls (priority order):

- Multi-factor authentication (MFA) on all accounts — email, banking, donor systems first
- Password manager — Bitwarden is free and open-source; deploy for all staff
- Automatic OS & software updates enabled on every device
- Endpoint protection (antivirus/anti-malware) software on all staff computers
- Email spam and phishing filtering — built into Microsoft 365 and Google Workspace
- 3-2-1 backup rule: 3 copies, 2 different formats, 1 stored offsite or in the cloud

Access management:

- Least privilege — give staff only the access they need for their specific role
- Formal offboarding checklist — revoke ALL access on every departure day
- Separate credentials for volunteers vs. paid staff
- Annual review of who can access which systems
- Two-person authorization for all large financial transactions

MFA: Your Single Highest-Impact Action

99.9% of automated account compromise attacks are blocked by MFA

(Microsoft Research)

MFA options — from good to best:

- SMS text codes — OK: better than nothing, but vulnerable to SIM swapping
- Authenticator apps (Microsoft/Google Authenticator) — RECOMMENDED: free, strong, and easy
- Passkeys / hardware keys (YubiKey) — BEST: fully phishing-resistant

Where to enable MFA — in this order:

1. **Email accounts:** All staff and board member email, immediately
2. **Banking & financial systems:** Any system that can authorize payments
3. **Donor database:** Protect donor personal information
4. **Cloud storage:** SharePoint, Google Drive, OneDrive
5. **Social media accounts:** Foundation Facebook, LinkedIn, X/Twitter

Building a Security-Aware Culture

Technology alone will not protect you. Your team is both your biggest risk and your greatest defence.

Staff training:

- Annual security awareness training (KnowBe4 and Proofpoint offer nonprofit pricing)
- Simulated phishing tests — practice before you are actually attacked
- Monthly security tips in staff meetings or via email
- Include board members and volunteers, not just paid staff

Policy & culture:

- Written acceptable use and password policy — simple, one page is fine
- Clear, easy process for reporting suspicious emails — remove barriers
- No-blame culture: celebrate reporting, never punish it
- Leadership must visibly model good security habits

KEY SHIFT: Security is a governance responsibility — it starts at the board, not the IT desk.

Incident Response

It is not IF — it is WHEN. Having a plan before an incident is the difference between a bad day and a disaster.

Before — Prepare:

- Written IR plan with contact list / Cyber insurance in place / Legal counsel identified
- Verify your backups actually restore / Staff trained on who to call first

During — Contain:

- Isolate affected devices immediately — unplug from network
- Do NOT pay ransom without consulting a professional incident response firm
- Preserve evidence — do not wipe systems / Notify IT support and leadership

After — Recover:

- PIPEDA breach notification if required — within 72 hours of discovery
- Notify affected donors and partners / Restore from verified clean backups
- Post-incident review / Update policies to prevent recurrence

Budget-Friendly Tools & Resources

Free or low-cost tools for nonprofits:

- Microsoft 365 for Nonprofits — email, Teams, Defender, MFA (free/donated via TechSoup Canada)
- Google Workspace for Nonprofits — Gmail, Drive, built-in security controls (free)
- Bitwarden — open-source password manager, trusted and free
- Have I Been Pwned (haveibeenpwned.com) — check if your email is in a known breach (free)
- CIRA D-Zone DNS Firewall — Canadian nonprofit DNS protection (low cost)

Canadian resources:

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

Table Discussion: Share Your Experiences

Choose one to discuss at your table:

1. Has your foundation experienced a cyber incident or near-miss?
2. What is your biggest cybersecurity challenge right now?
3. What security practice has worked well at your foundation?
4. What would help you most in the next 90 days?

Your 90-Day Action Plan

DAYS 1–30: Quick Wins

- Enable MFA on all staff and board email accounts
- Deploy Bitwarden (free password manager) for all staff
- Run haveibeenpwned.com audit on all work email addresses
- Test your backup: restore a file to verify it works
- Create a “who do we call?” incident response contact list

DAYS 30–60: Build Foundations

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

DAYS 60–90: Sustain & Improve

- Write your incident response plan (one page is enough)
- Present a security status update to your board
- Set a recurring annual security review date in your calendar

Shared reflections

What's one key takeaway or "AHA" that you want to remember?

What are you curious about now?

Individual Reflection

What tools & ideas can you take back to your community foundation board?

COMMUNITY FOUNDATION CONFERENCE

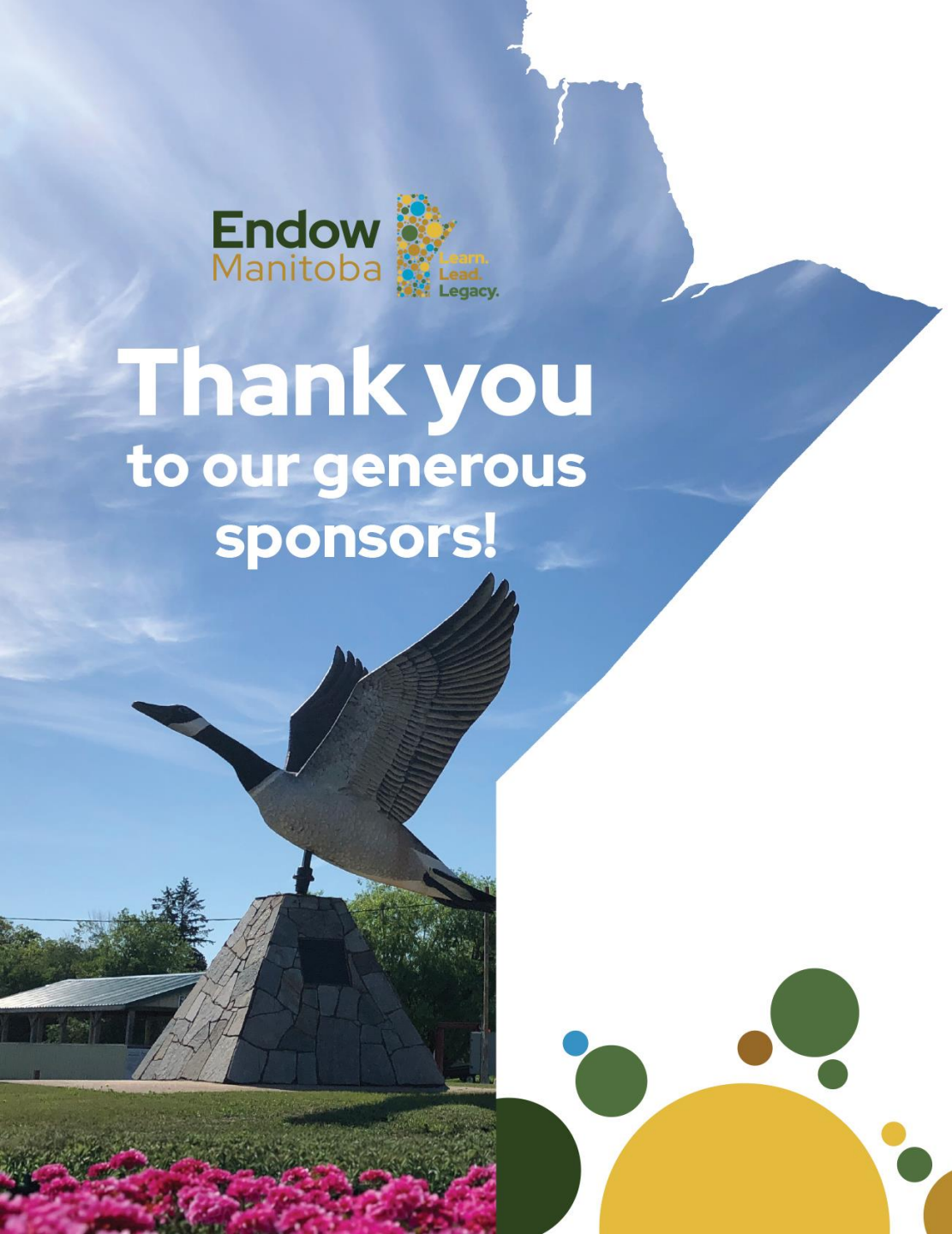
Endow Manitoba

Learn. Lead. Legacy.

APRIL 24 • 26, 2026

Thank you

Endow Manitoba a program of The Winnipeg Foundation



Endow Manitoba
Learn. Lead. Legacy.

Thank you
to our generous sponsors!

COMMUNITY FOUNDATIONS OF CANADA

CONNOR, CLARK LUNN
INVESTMENT MANAGEMENT

IFM Investors

TD Global Investment Solutions