TBN Computer Security Education

What TBN Directors and Club Admins must know

Target Audience

- All Board Members
- Everyone with a @tbn.ca Email account
- Everyone with Wild Apricot Admin privileges

Why?

- Board members are personally accountable for their actions/inaction
- Board is responsible to ensure that “staff” of club are aware of club policy.
- We all need to “protect” out Computer assets.

What to protect?

- Financial Assets
  - All corporate assets held via TD Bank account
  - PayPal account for on-line transactions
  - Wild Apricot/TBN stores no user credit card info
- Operational assets
  - websites (tbn.ca and tbnapplications.com)
  - Email (@tbn.ca is really Gmail)
- Data
  - member/contact data via websites
  - Routes via RideWithGPS

Why protect?

- TD Bank Account/PayPal access
  - Could steal TBN money
    - Lawsuits/Bankruptcy
- Wild Apricot
  - Could steal member data
  - Could host malicious content on our site
    - We could lose our site content (would take man years to recreate)
    - Reputational damage
    - Lawsuits
- Gmail/Google Drive
  - Loss of Corporate files/ability to run TBN
- RideWithGPS
  - We could lose our route information
    - Would be difficult to rebuild.

“Free” protection

- TD Bank/PayPal
  - Protects us if we protect our corp access
    - Computer/online credentials
    - “ATM” cards and PINs
- Wild Apricot (Personify)
  - Systems hosted (day-to-day running) by Personify
    - Security patches/software upgrades
    - Backups
- Gmail/Google Drive
  - Hosted by Google
  - SPAM filtering
- RideWithGPS
  - Back up routes and events every 7 day(s), keeping 12 backup(s).

Member/Contact Data

- Sensitive Personally Identifiable Information
  - Photo (opt)
  - Name
  - Home Address
  - Phone Number
  - Birthdate (opt)
  - Emergency Contact name and phone number
  - Occupation (opt)

Wild Apricot Admin/1

- Full Admin
  - technical@tbn.ca, treasurer@tbn.ca, webadmin@tbn.ca and president@tbn.ca
- Read only Full admin
  - secretary@tbn.ca
- Membership Manager (r/w member data)
- Event Manager (r/w member data)
- Restricted Website Editor

Wild Apricot Admin/2

- Who
  - All **Program Coordinators** + Cyclon (personal accounts)
  - Some board members
  - Some special event coordinators
- What
  - Event Manager
    - Write access to Member data, Event content
    - Send emails
    - Some Financial access
  - Restricted Web Site Editor
    - Write access to specific web pages

Technical Director

- Zendesk – RideWithGPS Helpdesk
- WildApricot.com – WA Support
- Namespro.com – DNS registration
- Surveymonkey.com
- GoDaddy.com
  - tbnapplications.com admin & custom web applications (Ride Leaders Report, etc).
- Zoom
- Others…

Passwords

- Hard
  - Long – at least 16 characters
  - Complex – upper/lowercase/number/special
- Avoid “guessable” passwords
- WA **does not** lock out after N failures
  - Vulnerable to brute force password guessing attack
- Unique – **do not use same password for TBN as you use on other sites.**
  - Don’t use the same for WA and Gmail.
  - Avoids cross compromise of passwords.

Passwords/2

- If you believe that your Gmail password is compromised, use Gmail recovery email and/or phone number. See
  - https://support.google.com/accounts/answer/32040
  - Technical director can reset your password.
- If you believe your WA password is compromised, contact technical@tbn.ca – or call me!

Examples of Secure Passwords

- n24WBGGL*dwe$R92
- oYDpy7mW7o*$7w8#
- #s54e7oz#Q*xG!8T

- Note: don't use these – they are examples of 16 character hard passwords!

Passwords/3

- Too many passwords?
  - Consider using a Password Manager/Vault
    - Examples:
      - 1Password
      - Bitwarden
      - LastPass

Vault Master Password

- Use a “Password Haystack”
  - Strength in length, yet with minimal complexity.
  - **Never** re-use anywhere else
  - https://grc.com/haystack.htm
- Example: (36 character haystack)
  - An.Apple@1day.keeps*the*dentist.Away
    - 507 hundred billion trillion trillion trillion years
  - 16 random string -> 141 hundred million years

Sharing Passwords

- Generate a strong random password.
- Save to your vault.
- Send password via disconnected channel without context (don't say "this is password for X" in message).
  - Via a text message, or
  - To a personal email account

Cyber Tips

- Keep your OS up to date
- Keep your browser up to date
- Don't even **access** TBN systems (email or WA) via public (unsecured/free) WiFi
  - E.g. Tim Hortons, Starbucks, TPL, etc.
  - Applicable for non-admin access too!
- Hide/Protect your passwords.

Cyber Tips/2

- Don’t click on unexpected attachments in email (even personal email)
- Consider using Anti-virus software

Sending Email

- Don’t share members’ personal email ids
  - Use BCC: instead of To: or CC:
  - It is okay to share @tbn.ca email ids.
- Send from @tbn.ca vs. <personal>.
  - Are you speaking in TBN role, or as yourself?

Board Members

- Use Shared Google Drive instead of email attachments.

tbnapplications.com

- Ride Leaders Report
- **All Wild Apricot admins** can Export a list containing all RLR which may contain sensitive info.
  - Read certification notice for details.
- Delete/protect these files after use.

Summary

- Never reuse passwords!
  - Don’t use the same password for @tbn.ca email as on www.tbn.ca
- Use random generated passwords everywhere:
  - At least 16 characters, mixed case, numbers, symbols
- Use a Password Vault with Master Password being a long Haystack
- Keep your OS etc. up to date

Thoughts on LastPass Breach

- Attackers copied an undisclosed number of customer vaults
- Site Passwords encrypted using Master Passwords, but URLs of sites in the vaults were visible (in plaintext).
- If you were a LastPass customer prior to Dec 22, your exposure is based on how hard your Master Password to guess. **Recommend:**
  - Review Haystacks example
  - Make sure you use a very hard MP.
  - Go to every account “of value” in the vault, and change/save the site password
  - Ensure **Password Iterations** (PBKDF2) is at least 100,100

Required End Page

TORONTO BICYCLING NETWORK