Website Security

Websites are valuable territory!

- If a cybercriminal can gain access to your website, they have a free online home for their malware, spam, advertisements, or phishing pages. These criminals are constantly searching for any website weak enough to take over!
- People who want to target your organization specifically can target your website. They can try to guess your credentials, find your password on a breach list, or use a botnet to overwhelm your website with traffic (a distributed denial of service or DDoS attack).
- Harassers targeting your organization can find photos and email addresses of board, staff, or volunteers to use in their harassment.

Luckily, there are ways to protect against all of these potential attacks!

Website Security Checklist

- ❏ SSL Certificate (the lock icon in the URL bar)
- ❏ Protect all forms with CAPTCHA (Google or hCaptcha) to prevent spam and protect your site from carding attacks
- ❏ Enable DDoS protection for free from either Deflect.ca, Project Galileo (Cloudflare), or Project Shield (Google)
- ❏ Everyone who needs access to the website should be provisioned their own account with a strong, unique password
- ❏ Enable two-factor authentication (require it if possible)
- ❏ Use contact forms instead of publicizing staff emails
- ❏ Create an update schedule and set up update notifications
    - ❏ Train and designate someone to update the website
    - ❏ Automate updates if possible
- ❏ Keep a list of essential website information in a secure place that at least two staff members can access
    - ❏ The list should include where the domain is hosted; a link to update the SSL certificate if it expires; and the link where you go to edit the website
    - ❏ Store website credentials separately, in a password manager
- ❏ Optional for extra privacy: use avatars instead of staff photos