Top 10
Security Tips to Keep Our Workplace Safe

1 Use Strong Passwords for Everything

Avoid easy ones like "Nonprofit123!"—use long, unique passwords for your email, CRM, and cloud tools.

2 Turn on Multi-Factor Authentication

This simple step adds major protection for your email, donor platforms, and accounting systems.

3 Don't Click Suspicious Donation or Volunteer Links

Hackers send fake donation emails. Always check the sender address and avoid clicking unknown links.

4 Stick to Organization-Approved Tools

Use the CRM, file storage, and email platform your nonprofit provides, not personal accounts or drives.

5 Be Careful with Donor and Beneficiary Info

Never store it in personal documents, share it over unencrypted email, or talk about it in public places.

6 Report Lost Devices Immediately

If your laptop, tablet, or phone goes missing, even if it's your personal one, let IT or your supervisor know right away.

7 Don't Share Logins (Even to "Help Out")

Everyone should use their own account. Sharing creates audit and security risks.

8 Keep Your Software Up to Date

Install updates when prompted. Many software updates include security improvements.

9 Limit Access to What People Need

Volunteers and interns should only access what's essential, not the whole donor database.

10 When in Doubt, Ask

Not sure if something's safe to click or share? Ask your tech lead, IT support, or supervisor before you act.

Learn more at **phinsecurity.com**