Nonprofit
Risk Management
Center
Find the answer here | nonprofitrisk.org

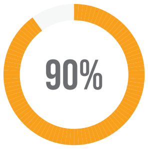
TIPS Cybersecurity Defense

Install and maintain up-to-date anti-virus software, firewalls, and email filters.

Use and enforce multi-factor authentication.

Protect against phishing (email), vishing (voice), and smishing (text) attacks. If a call, text, or email **SEEMS** suspicious, it **IS** suspicious.

Alert your team to the common indicators of phishing attacks: generic greetings and signatures, spoofed hyperlinks and websites, odd spelling and layout, and suspicious or unexpected attachments.



Did you know that an estimated **90%** of data breaches begin with phishing? Phishing is the gateway to 80% of all reported security incidents.

Familiarize your team with cybersecurity terms/risks, such as: hacker, attacker, intruder, malicious code, and vulnerabilities.

Know and use excellent password etiquette: use the longest password possible (8-64 characters), don’t reuse passwords, and don’t use words that can be found in any dictionary of any language in your passwords.

Never provide personal information unless you are absolutely certain that the person has authority to have that information.

Always check the security of a website before submitting personal information.

SOURCE: https://www.cisa.gov/uscert/ncas/tips/ST04-014