Password and Account Security Checklist

Protect your accounts with strong passwords and multi-factor authentication

19 items • nexusitnm.com

PASSWORD PRACTICES

- [ ] Use a password manager to generate and store unique passwords for every account.
- [ ] Use passwords of at least 16 characters for important accounts.
- [ ] Never reuse a password across multiple accounts.
- [ ] Never use personal information (birthdays, names, addresses) in passwords.
- [ ] Change passwords on any account where you have been notified of a data breach.
- [ ] Do not share passwords via text message, email, or chat.

MULTI-FACTOR AUTHENTICATION

- [ ] Enable multi-factor authentication (MFA) on every account that offers it.
- [ ] Prioritize MFA for email, banking, and any account tied to financial information.
- [ ] Use an authenticator app (such as Authy or Google Authenticator) instead of SMS when possible.
- [ ] Save your MFA backup codes in a secure location separate from your password manager.
- [ ] Do not approve MFA prompts you did not initiate -- this is a sign of an active attack.

EMAIL ACCOUNT SECURITY

- [ ] Secure your primary email account first -- it is the recovery method for all other accounts.
- [ ] Enable MFA on your email account.
- [ ] Review the apps and services that have access to your email and revoke any you do not recognize.
- [ ] Use a strong, unique password for your email that is not used anywhere else.

ONGOING ACCOUNT MANAGEMENT

- [ ] Review your accounts at haveibeenpwned.com periodically to check for breaches.
- [ ] Delete accounts for services you no longer use.
- [ ] Review active sessions on important accounts and sign out of devices you no longer use.
- [ ] Keep your recovery phone number and email address current on important accounts.

> This checklist is provided for informational purposes by Nexus IT Services, LLC. It is not a substitute for a professional security assessment. Contact us at (575) 263-6855 or nexusitnm.com if you need help implementing any of these items.