CYBER SECURITY

CHECKLIST

Phishing Protection

- Verify the sender before clicking links in emails or messages.
- Check for spelling errors or urgent language in emails—these are red flags.
- Never provide personal, including passwords or login information via email.
- Use a spam filter.

Data Privacy & Identity Protection

- Avoid publicly sharing sensitive details (SSN, student ID, address, phone number).
- Be cautious when filling out online forms; verify the source before submission.
- Use privacy settings on social media to limit who can see your information.
- Use strong, unique passwords and passphrases for different accounts.

Cybersecurity in Online Learning

- Use strong, unique passwords for your school accounts and online platforms.
- Log out of school portals and apps when using shared or public computers.
- Use strong, unique passwords and passphrases for different accounts.
- Use a virtual background or blur your background during video calls
- Be mindful of what is visible on your screen before sharing.

AI Security & Deepfakes

- Be cautious of AI-generated messages or videos that seem too good to be true.
- Verify sources of news, images, and videos to avoid misinformation.
- Do not share sensitive information with AI chatbots or AI Generative Tools.
- Avoid using AI-generated passwords or storing sensitive data in AI tools.
- Report any suspected deepfake scams to College Helpdesk passwords or storing sensitive data in AI tools.

Stay Safe Online

ALAMO COLLEGES DISTRICT
San Antonio College

Visit our IT Security Hub @ https://bit.ly/3E0iv4E

Need Help? Call: 210-486-0777

..... CYBER SECURITY CHECKLIST

Password & Account Security

- Use unique passwords for different accounts—never reuse old ones.
- Change your passwords every few months.
- Store passwords in a secure password manager, not on sticky notes.
- Log out of shared or public computers after use.

Wi-Fi & Network Security

- Avoid using public Wi-Fi for logging into sensitive accounts.
- Ensure your home router has a strong password and firmware updates.
- Never share your network password with untrusted individuals.
- Look for "HTTPS" in URLs when browsing or entering credentials. computers after use.

Social Engineering Awareness

- Be wary of messages or calls asking for personal details.
- Never share your student ID, Social Security number, or banking info with strangers.
- Verify the legitimacy of scholarships, job offers, or contests before engaging.
- Don't overshare personal information online—it can be used for identity theft.
- If something seems suspicious, confirm directly with your institution.

Mobile & Device Security

- Keep your phone and laptop operating systems updated.
- Install security apps and use biometric locks (fingerprint/Face ID.
- Enable remote tracking and wipe features in case of loss or theft.
- Do not download apps from unknown sources.
- Be cautious when granting apps permission to access your data.

Data Protection & Backup

- Regularly back up important files to a secure cloud or external drive.
- Encrypt sensitive documents before storing or sharing.
- Do not leave personal information visible on shared computers.
- Delete old accounts you no longer use to reduce risks.
- Be mindful of what personal information you share on social media.

Recognizing Security Incidents

- Unusual account activity (password resets, unauthorized logins).
- Phishing emails or messages asking for personal information.
- Malware infections (pop-ups, slow performance, unknown apps).
- Unauthorized access to school systems or files.
- Cyberbullying, online harassment, or inappropriate behavior in virtual spaces.

ALAMO COLLEGES DISTRICT
San Antonio College

Visit our IT Security Hub @ https://bit.ly/3E0iv4E
Need Help? Call: 210-486-0777