CYBER SAFETY

Back to school is right around the corner. It is time to purchase supplies and a new computer may be on the list may be new technology. Parents and students should be aware of the dangers of the internet including malware, phishing schemes, and safe computing practices.

Malware is commonly spread by users click on a link or malicious email attachment. Do not open attachments or click on links unless you are certain they are safe, even if the come from a person you know.

Emails and websites that appear to be legitimate may be malicious. Do not reveal personal information unless you are certain that it is needed for that website or you trust the email.

Keep the operating system, browser, and apps updated with patches. New machines out of the box should be immediately updated to ensure you are using the most secure software version.

Install antivirus with anti-phishing support and set the software to update automatically, running virus scans at least once a week.

Use caution with email attachments and untrusted links

Use caution when providing your information

Apply software updates and enable automatic updates

Create strong passwords

Install and use antivirus software

Keep passwords to yourself

Backup your data

BANK OF THE WEST
BNP PARIBAS

Threat Intelligence Group