Marshall County Schools

HACK PROOF HEADLINES

Think BEFORE You CLICK

Even your Google Calendars can be hacked!

The majority of Google Calendar scams involve links to fraudulent websites designed to trick you out of personal details: The classic digital con. These links can either be embedded in Google Calendar event descriptions, or in emails purporting to be Google Calendar invites: In both cases, a lot of care will be taken to make the links appear normal and genuine.

Stay Vigilant!

The usual advice for avoiding phishing attempts and social engineering scams applies here too. Be wary of anything coming into your inbox with a link embedded, even if it seems to come from Google Calendar or someone in your contacts list—and be particularly suspicious of anything out of the ordinary (like a lunch date out of the blue from an ex-colleague who left the company the previous year).

Unexpected Invitations

Following only invite links that you're expecting is a good general rule—you can always check directly with the sender of the invite if you're not sure—and if you find a link leads you anywhere other than Google Calendar, don't go any further. Even if you think you are on Google Calendar, double-check the browser address bar to make sure.

Double Check

You can dig deeper to check the origin of an email: In Gmail on the web, for example, click the three dots in the top-right corner of an email and Show original to see the full header information. This should include the full email address the invite has come from, and the sender field should read "calendar-notification@google.com" if it's an actual Google Calendar invite.

It is important to safeguard our school system and yourself by remembering to stay vigilant when clicking links embedded in emails.

Stop and think BEFORE you CLICK!

If you suspect deceit, hit delete!