

Gmail, Phishing and You

patricia falcon - 2023-10-23 - Comments (0) - Phishing

If you're unsure what is considered unsafe behavior when interacting with suspicious email, particularly as far as Gmail is concerned, this article is designed to answer your questions.

When is an email considered "opened", and is it safe to use Gmail's Preview function?

"Opening" an email is when you're viewing the email body. This includes viewing the email using [Gmail's preview function](#).

What are the risks of simply viewing an email?

Viewing an email is not inherently risky. At worst, the phisher/attacker knows that you've opened it. This is due to the use of what's called a "tracking pixel". This is a legitimate tool used by email delivery services to see if an email has been viewed. It's essentially an invisible image embedded in an email. The email references the image on a server that, when accessed, the sender knows that someone has viewed the email.

To prevent this, you can disable the "tracking pixel" by [turning off images in Gmail](#). However, this also prevents **all** images in email from being displayed, so as needed, you will need to reenable images to view them from trusted sources.

What actions are unsafe to take with a suspicious email and why?

Either downloading or accessing an attachment, clicking on a link, or responding to a request for information are all risky behaviors.

- Attachments can be purposefully misconfigured files that launch attacks on the computer they're opened on. Gmail does a good job in blocking these but it's an ongoing battle between malicious parties and email administrators on developing techniques in identifying harmful files.
- Links can direct you to sites that might take advantage of weak browser settings or even unknown vulnerabilities that could allow attackers access to a computer. Read [Keep Your Web Browsers Up to Date](#) and [Browse More Safely with an Ad Blocker](#) for protection tips.
- Replying to an email is also an avenue to phish for information. Warnings have been enabled in Gmail.com that alert users to properties about their emails that should be of note. You may notice that emails from non-Brown accounts have an "External" tag, or you've seen warning banners if an email says it's from a Brown account but isn't authorized correctly to do that (see [Gmail Anti-Spoofing Warning Banner](#) for details).

