TAC CIRA Email Service: How to Deal with SPAM & Phishing Emails

Recently, there has been an internet-wide increase in SPAM and phishing emails. Phishing emails attempt to trick the recipient by disguising the sender as a colleague, elected official or known person, in an attempt to penetrate networks, spread malware to or steal information from the email recipient. This is a widespread issue that is affecting state agencies, schools and municipalities.

This guide discusses the steps you and your staff when encountering SPAM or phishing emails.

Step 1: Think Before You Click

When you receive a suspected phishing email, it's **very important** not to click on any links, open any attachments or respond.

If you're uncertain whether an email from a colleague or friend is legitimate, call or visit the recipient in person to confirm they sent it.

Step 2: Report the Email to CIRA Support

Forward all suspected phishing emails to support@cira.state.tx.us so that we can blacklist the email addresses to prevent them from further communications to your county.

Step 3: Mark the Email as SPAM or Junk

Webmail Users

Click on "More" and then "Report Spam." You can also right click on any message in your inbox and then click "Report Spam."

We recommend using our Webmail portal to send/receive emails. To access Webmail, please go to, https://cira.mymailsrvr.com

Sign in with your email address and current email password. If you do not know your password, please call TAC CIRA at (800) 456-5974.

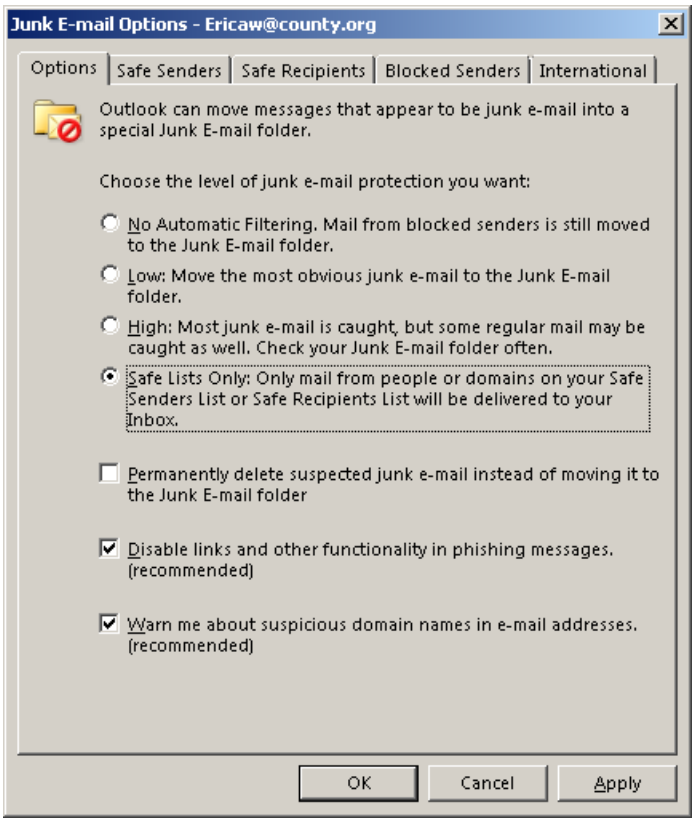
Outlook Users

Marking as Junk in Outlook

Click on the word "Junk." This will open a menu that will allow you to block an email sender and also update your junk settings.

Adjusting Your Junk Mail Options in Outlook

We recommend setting your "Junk Email Options" to the highest level. By default, Outlook is set to "no automatic filtering." We recommend updating this setting to "Safe Lists Only." We also recommend placing a check in the options for "Disable links and other functionality in phishing messages" and "Warn me about suspicious names in e-mail addresses" (last two options in the image below).



The link below will take you to an article that will assist you with updating your Junk email options: https://support.office.com/en-us/article/change-the-level-of-protection-in-the-junk-email-filter-e89c12d8-9d61-4320-8c57-d982c8d52f6b

Outlook Add-on for Reporting SPAM to Microsoft

There is a free add-on that you can download to report SPAM to Microsoft from within Outlook. More information and a download link can be found at: https://appsource.microsoft.com/en-us/product/office/wa104381180

Please consult with your county's IT staff before downloading.

Step 4: Ongoing Training for Staff

The easiest way to deal with a cyberattack is to prevent it from ever happening. Find information about TAC's free Cybersecurity Awareness Training Program here.