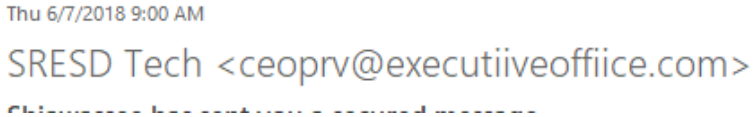
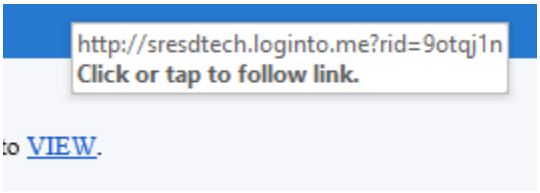
You have been Phished in a training exercise provided by the Shiawassee RESD Tech Department. The following is a list of items contained in the email that should have been clues that it was a Phishing email. In this training exercise no login or passwords were compromised there is no need to take action by changing your password.

1. From address – Pay special attention to the @domain.com this should have been from @shiawassee.net or SRESD.org if this was truly a legitimate email. Example below

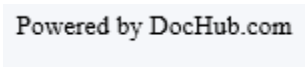


2. Were you expecting a secured document or encrypted email from the sender?

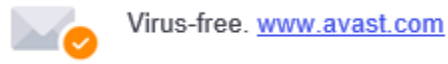
3. When hovering over a link or attachment in outlook it will show you the address it's forwarding/sending you to. Does it look legitimate?



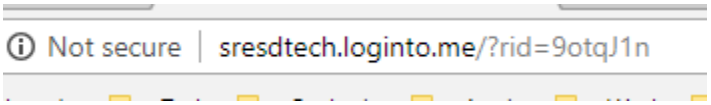
4. Is the application/website something you have received or utilized in the past?



5. Have you had any of the email/s the SRESD or County sent have/had an "avast.com" footer on them?



6. The link is clearly not secure. Any secure sites will utilize https:// not http://. Never enter any login credentials into a non-secure site. All credentials being sent in http:// is clear text and can be compromised.



Last thing is when in doubt don't click the link or attachment. Contact the helpdesk or person sending you the email over the phone to see if they really sent the following email. You can always forward a questionable email as an attachment to helpdesk@shiawassee.net for one of our tech's to analyze, to know how you should proceed.