Is this Legit? Email Safety Guide

Cyber scams like phishing are not only annoying, they pose serious risk of harm to our organization, our employees, and our students.

Hackers love to use email messages as a tool to get their hands on information they shouldn't have, such as your account information, password, and—worse yet—secure financial information or student data. This is called phishing. Don't fall for it!

Keep the following basic guidelines in mind, and you can be sure you are keeping your information—and the District's data—safe from cyber criminals.

Never trust an email if you don't know who sent it.

Always take a close look at the sender of the email. Does it end in @ easternpike.com? Do you recognize the address of the sender? If not, then you don't need to respond. Always err on the side of caution. Does it look like it came from someone you know, but you're not sure? You can always write or call that person and ask "did you send this to me?" Nobody will fault you for trying to be extra cautious.

Important to note: most email programs and web browsers use a display name and may not show the email address itself. For example, Outlook may show John Smith in your inbox, and the email is from john.smith@somewhere.com. You can usually hover with your mouse or double click on a display name to see what actual email address is behind it. This is very good practice, as hackers love to do things like send you a message from hacker@badguys.com and disguise it with a display name that looks legitimate like EASTERN HELPDESK. Always double and triple check where messages are coming from; it will keep you safe.

Never open or preview an attachment you weren't expecting to receive.

Cyber criminals may include a virus in an e-mail attachment and use a deceitful message to trick you into opening it, e.g. "Your e-mail account has been cancelled, see attachment for details." Viruses often have a .exe or .pif file extension, or they may be included in a .zip file. Even if the e-mail appears to be from someone you know, do not open or preview an e-mail attachment if you have any doubt that it is safe.

Never go to a link you don't recognize.

Hackers are getting more clever all the time. They may cut and paste our District's logo or something similar to make their message look legit. Look carefully at the address of the sender

and any addresses the message tells you to go to. Does it end in laud.net? If not, then that's a huge red flag that this message is probably a phishing scam.

Remember: a hacker may use display text that looks harmless but has something sinister hidden underneath. Most browsers and email programs allow you to hover over a link to reveal where it points to (usually toward the bottom of the window).

Never give out your password to anyone. Anyone!

Eastern will never, ever ask you to provide personal information such as your password in an email. We may remind you that it is time to change your password but it would come from t.keeton@easternpike.com. Is an email asking you to update your password and sending you to a link that doesn't end in easternpike.com? Then it's probably a phishing attack. Don't be tricked!

If an email does not "feel right"? Don't respond

With a little practice you can learn to spot phishing scams from miles away. For instance…

- Does the message have a high sense of urgency such as "respond now or we'll shut down your account!!!"?
- Does the text of the message have a lot of spelling or grammar errors or broken English?
- Is the message asking you to go to a non-Eastern website and enter personal information?

These are all major red flags. Learn to recognize them, delete any messages such as these, and you are on your way to being a well-informed email user keeping yourself and our students safe from cyber criminals.

Are you ever not sure if an email is legitimate? You can always double check by contacting t.keeton@easternpike.com