Valortech
A Veteran Owned Company

How to Spot a Fraudulent Phishing Email

Always use strong passwords.

It's always a good idea to have strong, complex passwords, and to not use the same password for more than one account or site.

Carefully hover (don't click!) over links and see if they go to a legitimate URL.

If the email is from Paypal, a link should lead back to paypal.com or accounts.paypal.com. If there is anything strange between 'paypal' and the '.com' then something is suspicious. There should also be a forward slash (/) after the .com. **Everyone handles their domains a little differently, but use this as a general rule of thumb:**

- paypal.com - *Safe*
- paypal.com/activatecard - *Safe*
- business.paypal.com - *Safe*
- business.paypal.com/retail - *Safe*
- paypal.com.activatecard.net - *Suspicious!*
- paypal.com.activatecard.net/secure - *Suspicious!*
- paypal.com/activatecard/tinyurl.com/retail - *Suspicious!*

*(*Don't trust dots after the domain!)*

*Remember!

...these tricks are designed to be subtle and easy to miss! Pay close attention to what you are clicking on!

- **Check the email in the header.** An email from Amazon wouldn't come in as noreply@amazn.com. Do a quick Google search for the email address to see if it is legitimate.
- **Always be careful opening attachments.** If there is an attachment or link on the email, be extra cautious. If the email shows up out of the blue with an attachment, even if it is from a sender you trust, it doesn't hurt to ask them if it is legitimate.
- **Be skeptical of password alerts.** If the email mentions passwords, such as "your password has been stolen," be suspicious.
- **Spread phishing awareness!** There is no shame in being over cautious! If you show those that you work with that you are mindful of these types of threats, they may adopt similar practices. In the long run, it makes email much safer for everybody!

valortech.io
sales@valortech.io
(414) 410-9440

10437 W. Innovation Dr
Suite 462
Wauwatosa, Wisconsin 53226