



RISKY THE ARMADILLO'S EMAIL SECURITY CHECKLIST

**THINK
BEFORE
YOU CLICK!**



Cut here and tape Risky to your computer as a daily reminder!

Risky the TML Risk Pool's mascot, the federal Cybersecurity and Infrastructure Agency, and the TML Risk Pool's Cyber Squad say "armor yourself against email phishing scams!" Stay safe with three simple tips:



Recognize

Look for these common signs:

- Urgent or emotionally appealing language, especially messages that claim dire consequences for not responding immediately
- Requests to send personal and financial information
- Untrusted shortened URLs
- Incorrect email addresses or links, like amazon.com

A common sign used to be poor grammar or misspellings, although, in the era of artificial intelligence, some emails will now have perfect grammar and spelling, so look out for the other signs.



Resist

If you suspect phishing, resist the temptation to click on links or attachments that seem too good to be true and may be trying to access your personal information. Instead, report the phish to protect yourself and others. Typically, you'll find options to report near the person's email address or username. You can also report via the "report spam" button in the toolbar or settings.



Delete

Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. Just delete.

CHECK OUT THE CYBER LIABILITY PAGE AT WWW.TMLIRP.ORG ►



THE TML RISK POOL'S CYBER SQUAD

CLICKED ON A BAD LINK AND GOT HACKED?
CONTACT THE POOL'S CYBER SQUAD
IMMEDIATELY AT 512-491-2300 OR
CYBERSQUAD@TMLIRP.ORG.



MIKE BELL
SENIOR
CYBERSECURITY
ADVISOR



RYAN BURNS
CYBER RISK
SERVICES
MANAGER

EAGER TO LEARN MORE? GO TO WWW.TMLIRP.ORG AND CLICK ON "CYBER LIABILITY" UNDER THE "RISK MANAGEMENT" DROP-DOWN MENU FOR CYBER PODCASTS, FREE VIRTUAL OR IN-PERSON CONSULTATIONS, AND MORE!