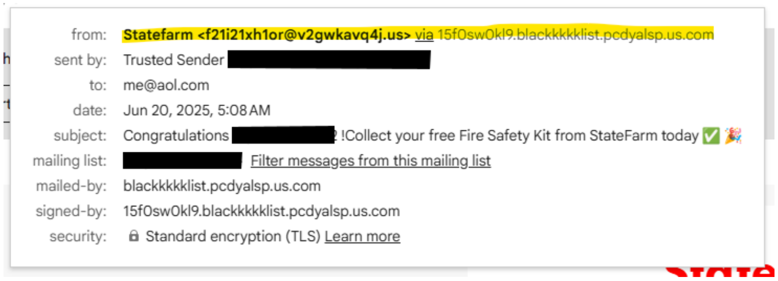
5 WAYS TO SPOT A PHISHING EMAIL

1. Suspicious Sender or Email Address

- The display name may look familiar (e.g., “Microsoft Support”), but the actual email address might be misspelled or from a suspicious domain (e.g., support@m1crosoft-secure.com).

Tip: Hover over the sender’s address to reveal the full domain before clicking anything.

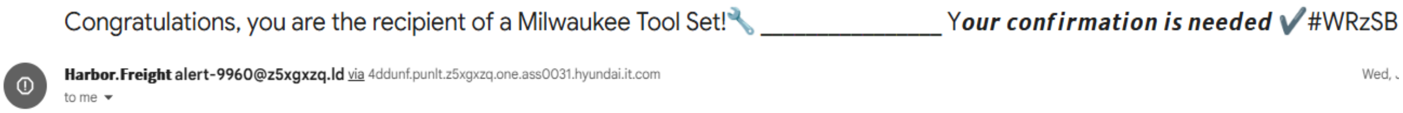


from: **Statefarm <f21i21xh1or@v2gwkavq4j.us>** via 15f0sw0kl9.blackkkkklist.pcdyalsp.us.com
sent by: Trusted Sender [redacted]
to: me@aol.com
date: Jun 20, 2025, 5:08 AM
subject: Congratulations [redacted] !Collect your free Fire Safety Kit from StateFarm today ✅ 🎉
mailing list: [redacted] Filter messages from this mailing list
mailed-by: blackkkkklist.pcdyalsp.us.com
signed-by: 15f0sw0kl9.blackkkkklist.pcdyalsp.us.com
security: 🔒 Standard encryption (TLS) Learn more

2. Generic or Unexpected Greetings

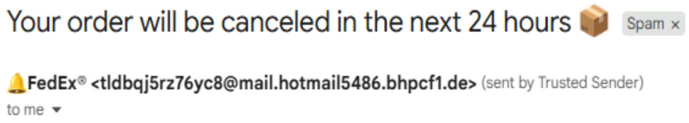
- Phishing emails often use impersonal language like “Dear User,” “Dear Customer,” or “Valued Client.”

Tip: If you’re used to personalized communication from an organization, a generic greeting can be a red flag.



Congratulations, you are the recipient of a Milwaukee Tool Set!🔧 _______________ Y***our confirmation is needed*** ✔️#WRzSB

Harbor.Freight alert-9960@z5xgxzq.ld via 4ddunf.punlt.z5xgxzq.one.ass0031.hyundai.it.com
to me ▾



Your order will be canceled in the next 24 hours 📦

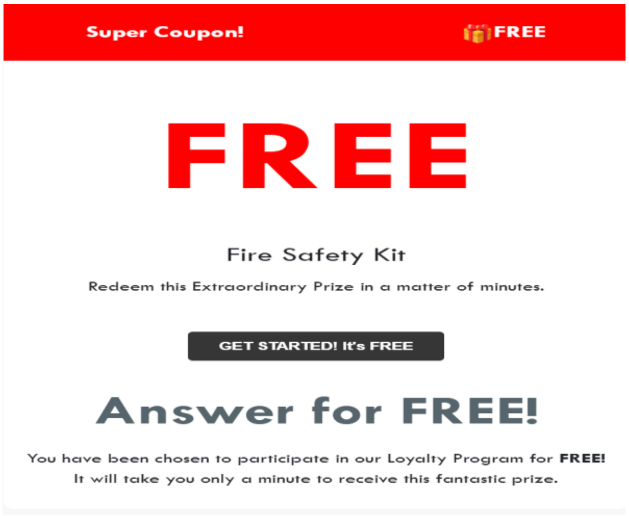
🔔**FedEx® <tldbqj5rz76yc8@mail.hotmail5486.bhpcf1.de>** (sent by Trusted Sender)
to me ▾

3. Urgent Language and Threats

- Phrases like “Act Now,” “Your account will be locked,” or “Immediate action required” are designed to create panic.
- Legitimate companies don’t pressure users into instant action without proper context or verification steps.

4. Unusual Links or Attachments

- Hover over links—if the URL looks strange, misspelled, or doesn’t match the organization’s official domain, don’t click it.
- Attachments with unfamiliar file types (e.g., .exe, .scr, .iso, or unexpected .zip) may contain malware.



Super Coupon! 🎁**FREE**

FREE

Fire Safety Kit

Redeem this Extraordinary Prize in a matter of minutes.

Answer for FREE!

You have been chosen to participate in our Loyalty Program for **FREE!**
It will take you only a minute to receive this fantastic prize.

5. Spelling, Grammar, or Formatting Errors

- Many phishing emails originate from attackers outside the targeted region and may contain awkward phrasing, poor grammar, or inconsistent formatting.
- Professional organizations typically proofread communications—multiple errors should raise red flags.