September 21, 2023

Hello Discount Tire Family,

We have seen an increase in phishing attempts targeting Our People through QR codes embedded in emails. These QR codes may appear legitimate but can lead to harmful consequences, including data breaches, malware infections, and unauthorized access to sensitive information.

What you need to know

Email “Phishing" is the most common type of cyber-attack that affects organizations like ours. Phishing attacks can take many forms, but they all share a common goal, getting you to share sensitive information, such as login credentials, credit card information, bank account details, or personal identity information.

IMPORTANT: To avoid these phishing schemes, please observe the following email Best Practices:

- Do not click on links or attachments or use QR codes from senders that you do not recognize.
- Always be aware of links, attachments and QR codes asking for usernames and passwords.

NOTE: Employee Benefit and Compensation emails will **only** be sent from Corporate Communications, Store Operations, Workday, or an email address from @discounttire.com.

- Be especially wary of .zip or other compressed or executable file types, such as .exe.
- Do not provide sensitive personal information (like usernames and passwords) over email; legitimate businesses will never ask for this information over email.
- Watch for email senders that use suspicious or misleading domain names.
- Inspect URLs carefully to make sure they are legitimate and not imposter sites.
- Do not try to open any shared document that you are not expecting to receive.
- If you cannot tell if an email is legitimate or not, please delete or let the Service Desk or Security know.
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

IMPORTANT: Hackers will often utilize names of individuals within your company, including Executives, or impersonate a real company to obtain your login credentials.

Our ask of you

- Please click on the following link: Cyber Attacks – Email Phishing Schemes and become familiar with the different phishing variations. This document can also be accessed from the Security page on the KC under Alerts.
- If you encounter any suspicious emails with QR codes or believe you have received a phishing attempt, please report it immediately by clicking the report phishing button. Our security team will investigate and take appropriate action to mitigate potential risks.

NOTE: If you receive a suspicious email, inadvertently click on a link, or open an attachment from an unknown source, please contact the Service Desk x66008 so the appropriate teams can review and respond.

Thank you for helping to keep Discount Tire's information safe!