# ITS Communications

Algonquin College
**Cybersecurity Awareness Month**
2024

## Phishing Emails Referencing HR Initiatives

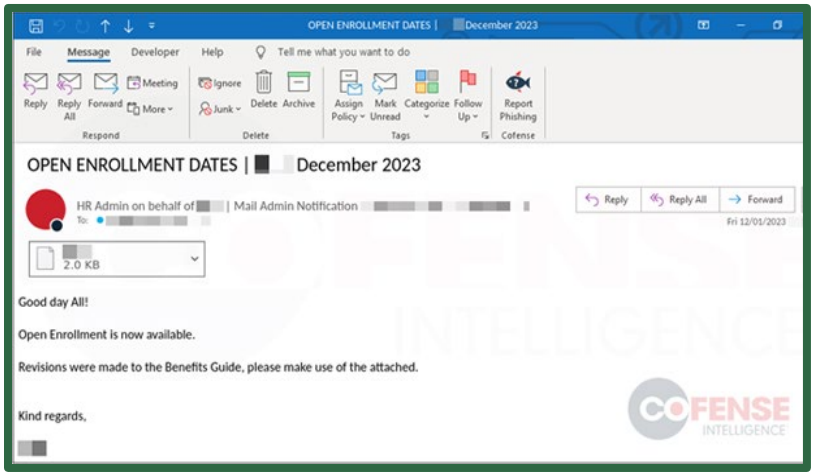
Be on the lookout for phishing emails referencing HR initiatives and tasks like open enrollment, CRA updates, salary adjustments, benefits changes, and employee satisfaction surveys as lures to steal credentials.

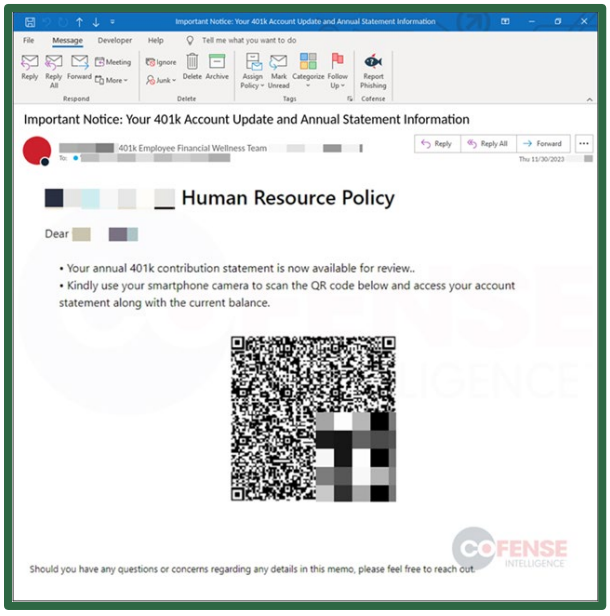
Phishing emails referencing HR initiatives are increasing in popularity since employees often expect to receive these types of emails at least once a year.

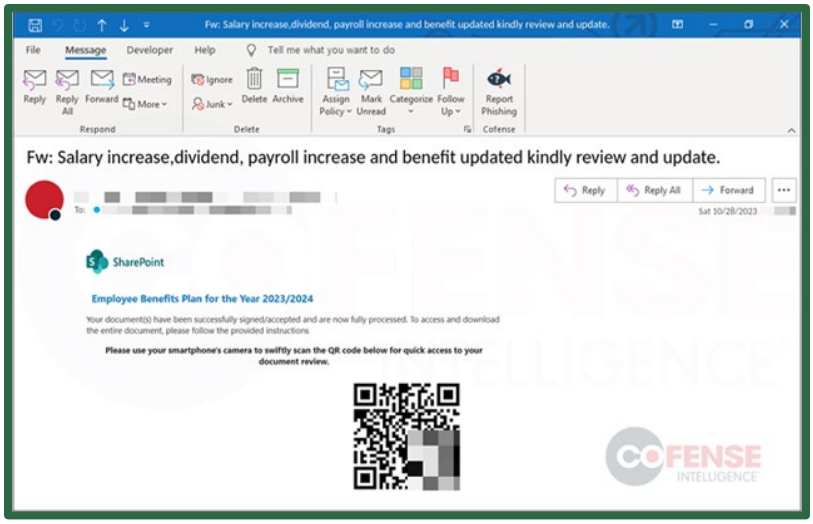
These HR tasks appeal to your emotions whether they are an exciting change in finances or benefits, an urgent task, or extra work to complete. This added emotion can cloud even the most well-trained employee's judgment when it comes to phishing emails. It's important to stay vigilant and remember the tips below:

1. **Don't click** links, open attachments, scan unexpected QR codes, or provide credentials. If the email is malicious this will allow attackers to infect your computer with malware or steal your information.
2. **Be skeptical of urgent requests** that do not follow typical company procedures and policies.
3. **Always verify.** If you know the sender, follow up with a quick phone call.

**REAL EXAMPLES OF PHISHING EMAILS BELOW**




**Remember, you are the last line of defense against phishing.**
**IF YOU RECEIVE A SUSPICIOUS EMAIL, REPORT IT IMMEDIATELY.**

Report Phishing

*Information Security & Privacy is Everybody's Business*