March 2023 – Phishing Results

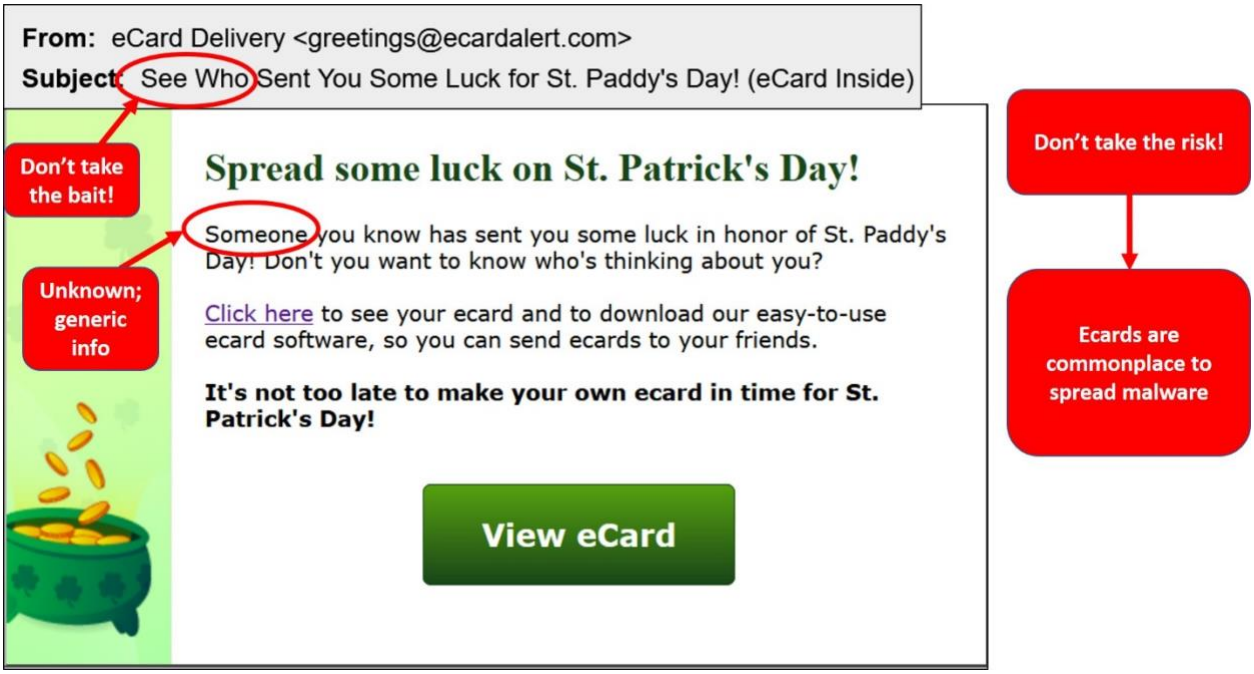
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *See Who Sent You Some Luck for St. Paddy's Day!*. The email scenario included a link to "view" the eCard. Ecards are used by attackers to spread malware. In this type of scam, the link leads to a website that prompts the user to download the ecard which may contain malware. It is difficult to distinguish between legitimate and malicious ecard emails. A simple rule to follow is to **not** take the risk, especially while using MC information technology resources (network and email).

Good news:
766 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

Opportunities for improvement:
188 employees clicked the link within the training email. One is one too many - one click puts the entire MC network at risk!

Did you click? In a real-world phishing attack clicking the link may have prompted you to give up your login credentials.

Please review the red flags within this type of phishing attack and to learn ways to spot a suspicious email.



What should you do if you suspect an email may be a phishing attempt?

Let IT Security analyze the email for you - **REPORT** the email! The Report Phishing button within your email client allows you to quickly report suspicious emails to IT Security. Learn how to

access the Phishing Reporter button when using Office 365 at home. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

If you have any questions or concerns, please contact the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT's web page
- by phone at 240-567-7222

Please do not reply to this email, as this mailbox is not monitored. Thank you.

IT Communications
Office of Information Technology