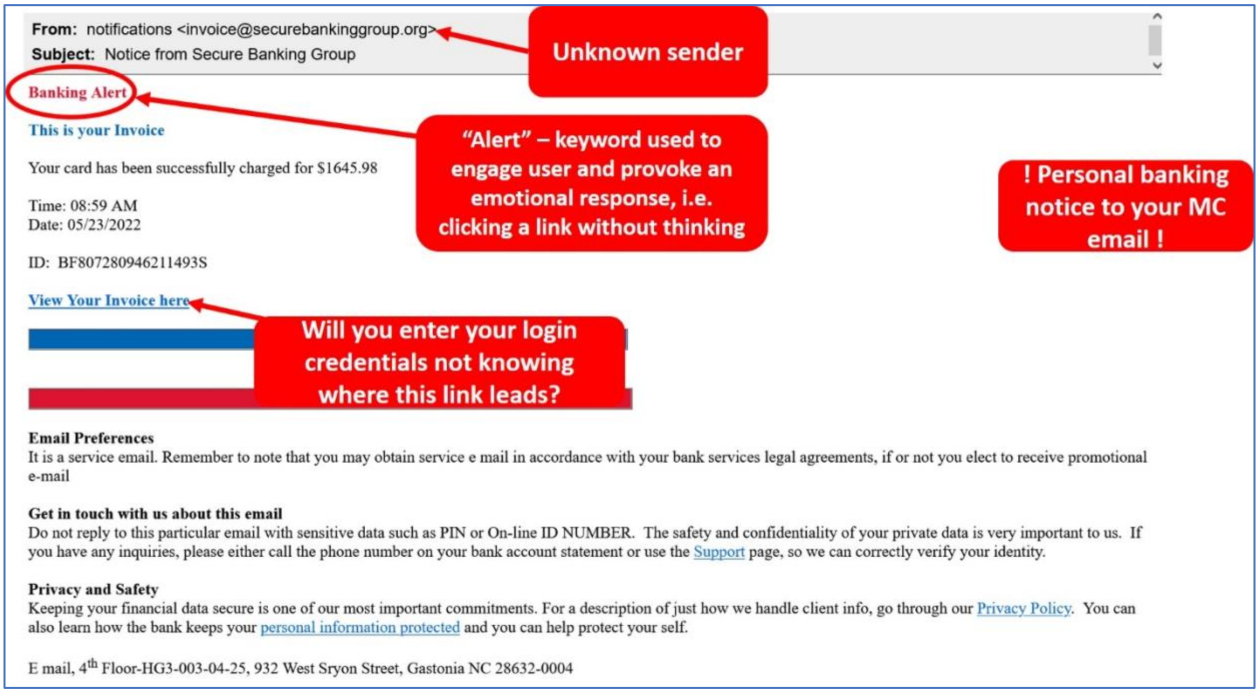
May Phishing Results: Banking Alert Invoice

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Notice from Secure Banking Group*. This scenario implied an automatic payment had been charged to your bank account. Automatic payments are a convenience however, attackers try to catch you off-guard knowing that you may forget what accounts are enabled for automation. The "set and forget" convenience is the path the attacker uses in hopes that you will click the link to inquire. This phishing threat is usually successful in gaining prompt action from the recipient.

1078 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

101 employees clicked the link within the training email. **Did you click?** *In a real-world phishing attack clicking the link may have prompted you to give up your personal banking credentials.*

Please review the clues within the email to help you identify this message as suspicious.



From: notifications <invoice@securebankinggroup.org>
Subject: Notice from Secure Banking Group

Banking Alert

This is your Invoice

Your card has been successfully charged for $1645.98

Time: 08:59 AM
Date: 05/23/2022

ID: BF807280946211493S

View Your Invoice here

Email Preferences
It is a service email. Remember to note that you may obtain service e mail in accordance with your bank services legal agreements, if or not you elect to receive promotional e-mail

Get in touch with us about this email
Do not reply to this particular email with sensitive data such as PIN or On-line ID NUMBER. The safety and confidentiality of your private data is very important to us. If you have any inquiries, please either call the phone number on your bank account statement or use the Support page, so we can correctly verify your identity.

Privacy and Safety
Keeping your financial data secure is one of our most important commitments. For a description of just how we handle client info, go through our Privacy Policy. You can also learn how the bank keeps your personal information protected and you can help protect your self.

E mail, 4th Floor-HG3-003-04-25, 932 West Sryon Street, Gastonia NC 28632-0004

Unknown sender

"Alert" – keyword used to engage user and provoke an emotional response, i.e. clicking a link without thinking

! Personal banking notice to your MC email !

Will you enter your login credentials not knowing where this link leads?

Report Phishing MC

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.

Follow these additional tips to avoid phishing scams:

- Do not user your MC email address for personal business. Separate your personal business from MC business.
- Check your emotions. Do not be curious and investigate the link – REPORT the email.
- Keep your MC business limited to your MC email address and use your personal email address for personal business.
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- Trust your instincts. If the email content, sender, and link or email attachment seems suspicious, do not open it. Play it safe and **REPORT** it.

If you have any questions or concerns regarding this process, 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