

## Phishing Scenario Results: Account Update February 2023

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Safety Account Information*. The email scenario directed the recipient to click a link to “verify” an email account. Account updates or verification request phishing emails are used as bait to capture login credentials. This is the easiest and most common social engineering trick used as no sophistication is required. The attacker simply “asks” for your login password. Your best defense is to report suspicious emails, especially requests for your account “verification”!

**Good news: 978 employees reported** the phishing scenario to the Phishtrap. **Nice work MC!**

**Opportunities for improvement: 20 employees clicked the link within the training email; of these individuals, 5 entered their credentials.**

**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.

The diagram shows an email interface with several red callout boxes pointing to suspicious elements:

- Unknown domain:** Points to the sender information: **From:** Account <accounts@verifytoken.com> **Subject:** Safety Account Information.
- Security info update:** The main heading of the email.
- Hover your mouse over the link to reveal the web address:** Points to the blue text **CLICK TO VERIFY**.
- What email account needs updated? Very generic / vague request!:** Points to the body text: **Dear User, Your email account has to be updated to avoid deactivation or Risk of theft.! So we strongly recommend that you should immediately verify your email account.**
- Spelling and Grammar mistakes are one clue:** Points to a red circle around the word **browse** in the warning: **WARNING! Protect your privacy. Log-out when you are done and completely exit your browse.**

The email body also includes a URL: <https://s.verifytoken.com/107519/aadcbc/de176f0a-3b7a-4e50-babf-74a99e4bab62/> and the instruction: **Click or tap to follow link.**

At the bottom, there are links for [Privacy](#) | [Legal](#) and [Unsubscribe](#) | [Unsubscribe Preferences](#).

**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](mailto: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