Office of the Chief Information Security Officer
RISK ADVISORY: BEST PRACTICES FOR MASS EMAIL

ciso.uw.edu

BACKGROUND

In order to mitigate the risks of phishing, the UW Office of the CISO recommends the following best practices for using links and link tracking in mass email messages sent to members of the UW community via various marketing platforms. Those who send messages directing users to web sites are also advised to avoid sending links to UW NetID login pages.

BEST PRACTICES

There is no perfect solution to the complex set of problems that allow cybercriminals to continue tricking users into giving up login credentials and, in some cases, exposing University and personal data. However, following some best practices in sending messages might help reinforce security-oriented habits.

1. Turn off link tracking in emails generated by marketing platforms. Also turn off "view email as a webpage."

2. Don't ask users to enter password credentials in login pages linked from email. Instead, direct them to a landing page where they can read more and understand the necessary context before entering their credentials.

3. Train users to regard emails that solicit information of any kind with suspicion.

4. Advise users to be wary of emails that create a false sense of urgency, such as those that admonish you to verify or update information or threaten to delete your account.

5. Use default statements such as "This email from UW-IT does not ask you to log in to a website" in the footer of your messages.

THE PROBLEM WITH TRACKING LINKS

In phishing awareness training, one of the defensive measures recommended to users is to hover over links in email to make sure the link and the destination are the same. Including tracking links in messages makes it difficult for recipients to follow this guidance with confidence.

In emails generated by marketing platforms, by default each link is tracked. The tracking code “cloaks” the URL in a way that makes it unrecognizable.

For example, a “cloaked” link may look like this:
https://discover.uw.edu/ab0cdefgh002trackyou

But then it redirects to a different web page, such as
https://ciso.uw.edu/abc

If users are trained to click on links that don't match the destination URL, they may lose the sense of vigilance needed to detect links that lead to malicious URLs.

For this reason, it is recommended to turn off tracking links. Turning them off will mean that data about users and which web pages they visited will not be available in reports attached to the marketing platform, but that information may be obtained by using other tools, such as Google Analytics.

LINKS TO UW NETID LOGIN PAGES

University Privacy Policy (APS 2.2) states that University workforce members shall not:

- Send unsolicited email (where the recipient has not granted permission for the message to be sent) to individuals that asks them to reply with confidential information, or

- Send unsolicited emails to individuals that ask them to click embedded links to University web self-service transactions that require entry of confidential information.

Please note that "confidential information" includes credentials such as UW NetIDs and passwords.

The policy further states that
"Unsolicited email does not include email sent from a University unit...to individuals who receive services from, or have an ongoing relationship with, the unit."

UW Office of the CISO, June 2018