Don't Get Tricked by Phishing Scams or Social Engineering

Summary

Some general advice about fraudulent emails

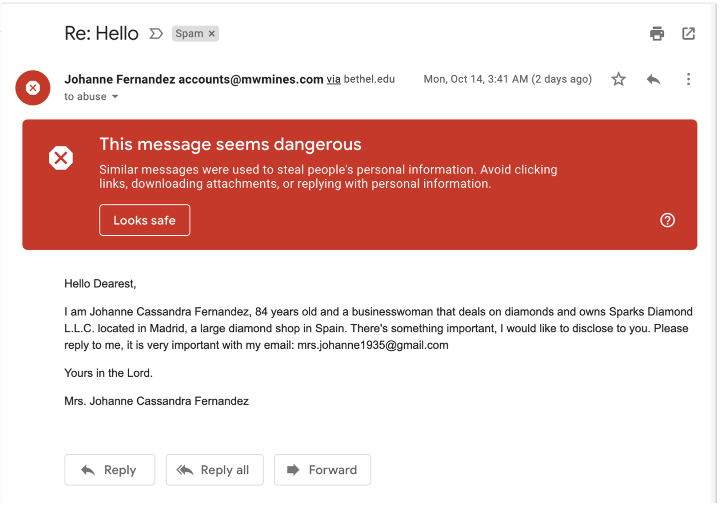
Phishing...not fishing

From time to time Bethel community members receive fraudulent emails from phishing scams. These misleading emails contain links to counterfeit websites or present requests that are designed to trick the reader into providing personal information. Sometimes these types of email scams appear to be coming from Bethel addresses, making them difficult to detect (through a process known as "Spoofing").

Here are some ways to protect yourself against fraudulent emails:

- **Be Alert:** no one at Bethel will ask you to share your password except through a Bethel authentication window that you have opened to access a specific Bethel resource.
- **Be Suspicious:** Look for signs that the email is a scam, such as it is not coming from a Bethel email address, the URL link is not a Bethel web address, and the subject line or greeting does not fit Bethel’s style.
- **Type, Don’t Click:** The only safe way to access an online account is by typing the website address directly into your browser or by using a bookmark if you have created because you regularly use the site. If you receive an email link to a website requesting your username, password, account number, social security number, or other personal information, do not click on it.
- **Ask Questions:** If you receive a suspicious communication of any form, please bring it to the attention of the Help Desk at helpdesk@bethel.edu or (651) 638-6500. Use Gmail's built-in Spam and Phishing report features to securely handle the scam email and to help improve our overall security posture. Every reported email helps Google to provide better "machine learning" analytics to continually provide better protection.

Gmail is here to help. Below is an example of a Phishing email. It uses a process known as Social Engineering to try and trick users into providing information. Notice the banner Gmail placed on the header of the email:



Re: Hello

Johanne Fernandez accounts@mwmines.com via bethel.edu Mon, Oct 14, 3:41 AM (2 days ago)

to abuse

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Hello Dearest,

I am Johanne Cassandra Fernandez, 84 years old and a businesswoman that deals on diamonds and owns Sparks Diamond L.L.C. located in Madrid, a large diamond shop in Spain. There's something important, I would like to disclose to you. Please reply to me, it is very important with my email: mrs.johanne1935@gmail.com

Yours in the Lord.

Mrs. Johanne Cassandra Fernandez

If you think your Bethel account has been compromised, please go to: https:// iam.bethel.edu, login and change your password. IAM at https://iam.bethel.edu is the **only** place you should ever change or reset your Bethel account credentials. Then please contact the Help Desk at helpdesk@bethel.edu or 651.638.6500.

Social Engineering

Social engineering is using readily available resources to convince someone that something is credible - social media is a huge repository of this, but so are news alerts, publications or even websites like the bethel directory.

Bad actors may use public details about you to "hook" you into their message. This may be through leveraging your position, your department, your major or even your faith to try and convince you they are both credible and that you should do something they are looking for (clicking a link, sending money, replying to an email).