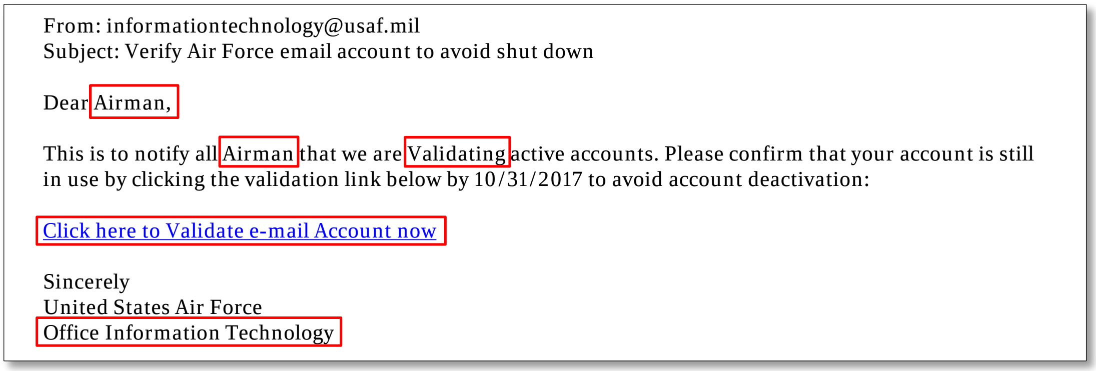
Spot The Phish

U.S. Air Force
Chief Information Security Office (CISO)



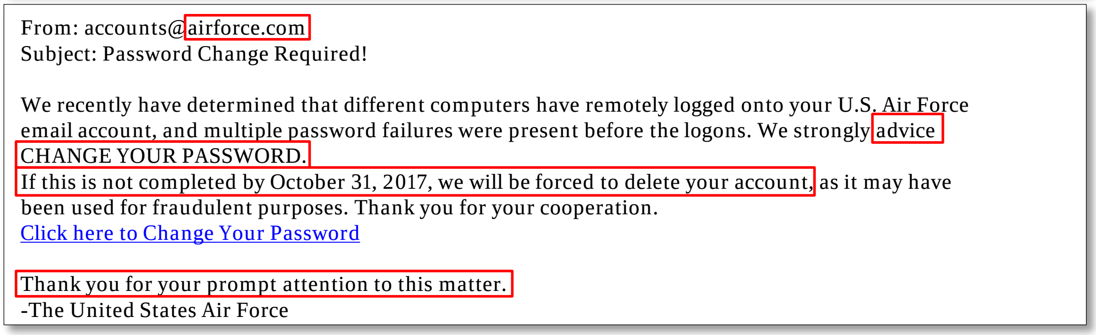
From: informationtechnology@usaf.mil
Subject: Verify Air Force email account to avoid shut down

Dear Airman,

This is to notify all Airman that we are Validating active accounts. Please confirm that your account is still in use by clicking the validation link below by 10/31/2017 to avoid account deactivation:

Click here to Validate e-mail Account now

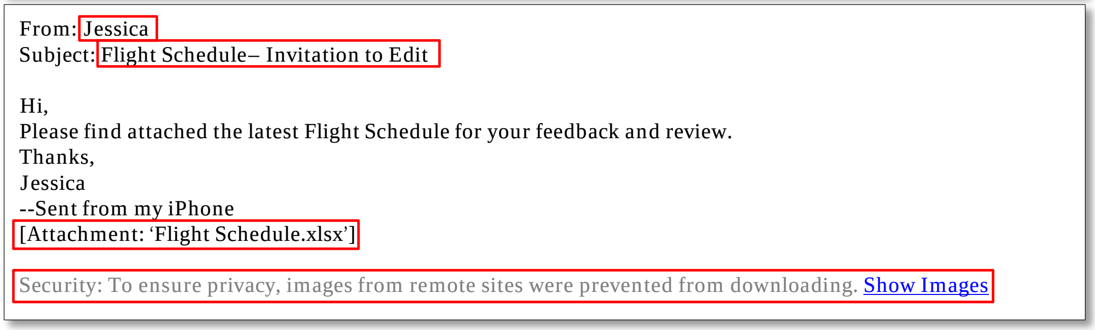
Sincerely
United States Air Force
Office Information Technology



From: accounts@airforce.com
Subject: Password Change Required!

We recently have determined that different computers have remotely logged onto your U.S. Air Force email account, and multiple password failures were present before the logons. We strongly advice CHANGE YOUR PASSWORD.
If this is not completed by October 31, 2017, we will be forced to delete your account, as it may have been used for fraudulent purposes. Thank you for your cooperation.
Click here to Change Your Password

Thank you for your prompt attention to this matter.
-The United States Air Force



From: Jessica
Subject: Flight Schedule– Invitation to Edit

Hi,
Please find attached the latest Flight Schedule for your feedback and review.
Thanks,
Jessica
--Sent from my iPhone
[Attachment: ‘Flight Schedule.xlsx’]

Security: To ensure privacy, images from remote sites were prevented from downloading. Show Images

Why is it phishy?

- Generic use of ‘Airman’
- Grammar mistakes
- Inconsistent capitalization
- Suspicious link

- Sender name/email address is illegitimate
- Spelling mistakes
- Email looks unprofessional
- Unusual sense of urgency

- Sender name is incomplete or “off”
- Contains suspicious attachment(s)
- Images were blocked by email filter

Tips and Tricks

Unsigned Email
For internal emails, ensure all messages are digitally signed by looking for the red ribbon icon. A digital signature indicates that no third party has intercepted the communication.

Double-check Links
To ensure accuracy of a URL prior to engaging, hover over the link.

Generic Audience
Be wary of emails that address a generic audience, such as “Airmen” or “client,” instead of a specific name.

Update Your Software
Ensure that your equipment system is up-to-date to help identify and block malicious programs.

Urgent or Threatening Content
Any email that is threatening or has an unusual sense of urgency should be approached carefully.

Scan for Malware
Verify the safety of all attachments contained in an email by scanning for malware.

Unexpected Content
Be cautious when interacting with messages unexpected senders or content.

Verify Sender
If a message from someone you know seems out of character, contact them via phone. The sender’s account may have been hacked.

Report any suspected phishing emails to your local Client Support Technician (CST) or Cybersecurity Liaison (CSL)