Phishing Email Examples

Taking the mystery out of

identifying a phishing message

Phishing Example #1

From: **IT Team** <IT@goshen.edu>
Date: Tue, Sep 19, 2023 at 2:41 PM
Subject: Suspicious Web Activity
To: <gretta@goshen.edu>

Invalid email address

All communication from ITS comes from either **helpdesk@goshen.edu** or **servicedesk@goshen.edu**

Dear Gretta,

We have introduced a new web trafficking monitoring service due to increased cybersecurity threats.

Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per the Acceptable Use Policy.

We do realize that this type of activity is often caused by viruses and other types of malware. Our detective and preventive controls blocked the malicious activity successfully. However, we would like you to review the site listing and let us know if any of these sites are legitimate to carry out your regular work.

https://activity-check.net/1457

This file is an .html file and can be opened with Google Chrome, Microsoft Edge, or Internet Explorer.

If you believe that any of the sites listed in the report have been reported erroneously or that all sites noted are false positives, please reply to this email.

Thank you,
IT Team

From: **IT Team** <IT@goshen.edu>
Date: Tue, Sep 19, 2023 at 2:41 PM
Subject: Suspicious Web Activity
To: <gretta@goshen.edu>

Subject line places emphasis on something that is really important. Or something that is meant to evoke a quick response from you.

Dear Gretta,

We have introduced a new web trafficking monitoring service due to increased cybersecurity threats.

Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per the Acceptable Use Policy.

We do realize that this type of activity is often caused by viruses and other types of malware. Our detective and preventive controls blocked the malicious activity successfully. However, we would like you to review the site listing and let us know if any of these sites are legitimate to carry out your regular work.

https://activity-check.net/1457

This file is an .html file and can be opened with Google Chrome, Microsoft Edge, or Internet Explorer.

If you believe that any of the sites listed in the report have been reported erroneously or that all sites noted are false positives, please reply to this email.

Thank you,
IT Team

From: **IT Team** <IT@goshen.edu>
Date: Tue, Sep 19, 2023 at 2:41 PM
Subject: Suspicious Web Activity
To: <gretta@goshen.edu>

🚩 Typically you can expect ITS to make an announcement in the Campus Communicator or Faculty Staff Bulletin to support email announcements.

Dear Gretta,

We have introduced a new web trafficking monitoring service due to increased cybersecurity threats.

Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per the Acceptable Use Policy.

We do realize that this type of activity is often caused by viruses and other types of malware. Our detective and preventive controls blocked the malicious activity successfully. However, we would like you to review the site listing and let us know if any of these sites are legitimate to carry out your regular work.

https://activity-check.net/1457

This file is an .html file and can be opened with Google Chrome, Microsoft Edge, or Internet Explorer.

If you believe that any of the sites listed in the report have been reported erroneously or that all sites noted are false positives, please reply to this email.

Thank you,
IT Team

From: **IT Team** <IT@goshen.edu>
Date: Tue, Sep 19, 2023 at 2:41 PM
Subject: Suspicious Web Activity
To: <gretta@goshen.edu>

🚩 **A request for you to take action on something that doesn't quite make sense**

Dear Gretta,

We have introduced a new web trafficking monitoring service due to increased cybersecurity threats.

Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per the Acceptable Use Policy.

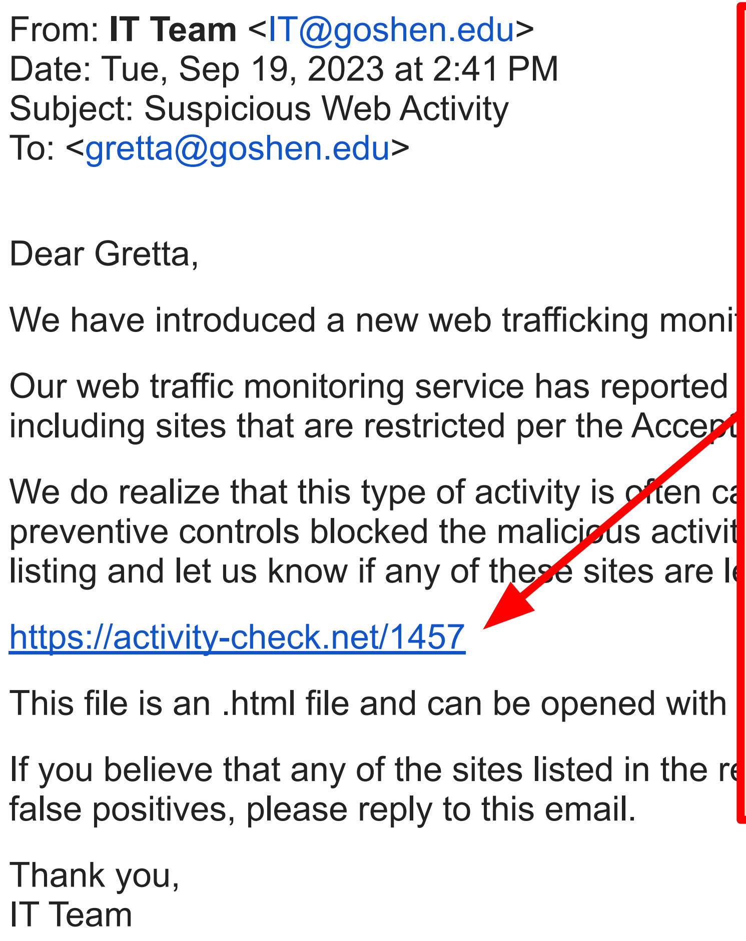
We do realize that this type of activity is often caused by viruses and other types of malware. Our detective and preventive controls blocked the malicious activity successfully. However, we would like you to review the site listing and let us know if any of these sites are legitimate to carry out your regular work.

https://activity-check.net/1457

This file is an .html file and can be opened with Google Chrome, Microsoft Edge, or Internet Explorer.

If you believe that any of the sites listed in the report have been reported erroneously or that all sites noted are false positives, please reply to this email.

Thank you,
IT Team



From: **IT Team** <IT@goshen.edu>
Date: Tue, Sep 19, 2023 at 2:41 PM
Subject: Suspicious Web Activity
To: <gretta@goshen.edu>

Dear Gretta,

We have introduced a new web trafficking moni

Our web traffic monitoring service has reported
including sites that are restricted per the Accep

We do realize that this type of activity is often ca
preventive controls blocked the malicious activit
listing and let us know if any of these sites are le

https://activity-check.net/1457

This file is an .html file and can be opened with

If you believe that any of the sites listed in the re
false positives, please reply to this email.

Thank you,
IT Team

🚩 A suspicious link

Hovering your mouse over the link reveals that you would be taken to a suspicious webpage

“https://05kqatnrj9s0snah9.phish.farm/XTkV0eGMxUlRTbUpvTTJjMlZqbGFNSHBFZHpoS1FreERVR2xsWTJSSVV6ZENTV2RCVDJwdWFtdHRRMk16T0hOa2JFeEJjM0ZvSzBaRWF6QnlWbFZqSzJOUk1VaHVWWVdhvTjNWTVJtaEhXRnBaVW05VkwxaFRSRzVLVlW5KcmVWRlNia2h1Ym5jelExZzBVamRIV2trclJGcEtjamxDVDNGQlkyRjBhMmw0Y1RGcFVVNXRPR0pvVTXpKYVNHNDRPQzk2UjIwemNqZExVakJqVEdaalFWVnJWp4UWs0MGRFVjZOMko2WWl0dmNNVeHBaemxvVEV4dGNtxUMFZWUWxRNUxTMXJZVEZQTW5rNFZIOUpiakZVVlZlZSSFVWSjVUbIlzUFQwPS0tOWY3NmYxOWZlMWI2MDg5NWE0ZTQ3ODg3YThjMTBmOWM3OWRkOWQyOQ==?cid=1709052202”

From: **IT Team** <IT@goshen.edu>
Date: Tue, Sep 19, 2023 at 2:41 PM
Subject: Suspicious Web Activity
To: <gretta@goshen.edu>

🚩 **An extraneous statement to try to bring legitimacy to the message**

Dear Gretta,

We have introduced a new web trafficking monitoring service due to increased cybersecurity threats.

Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per the Acceptable Use Policy.

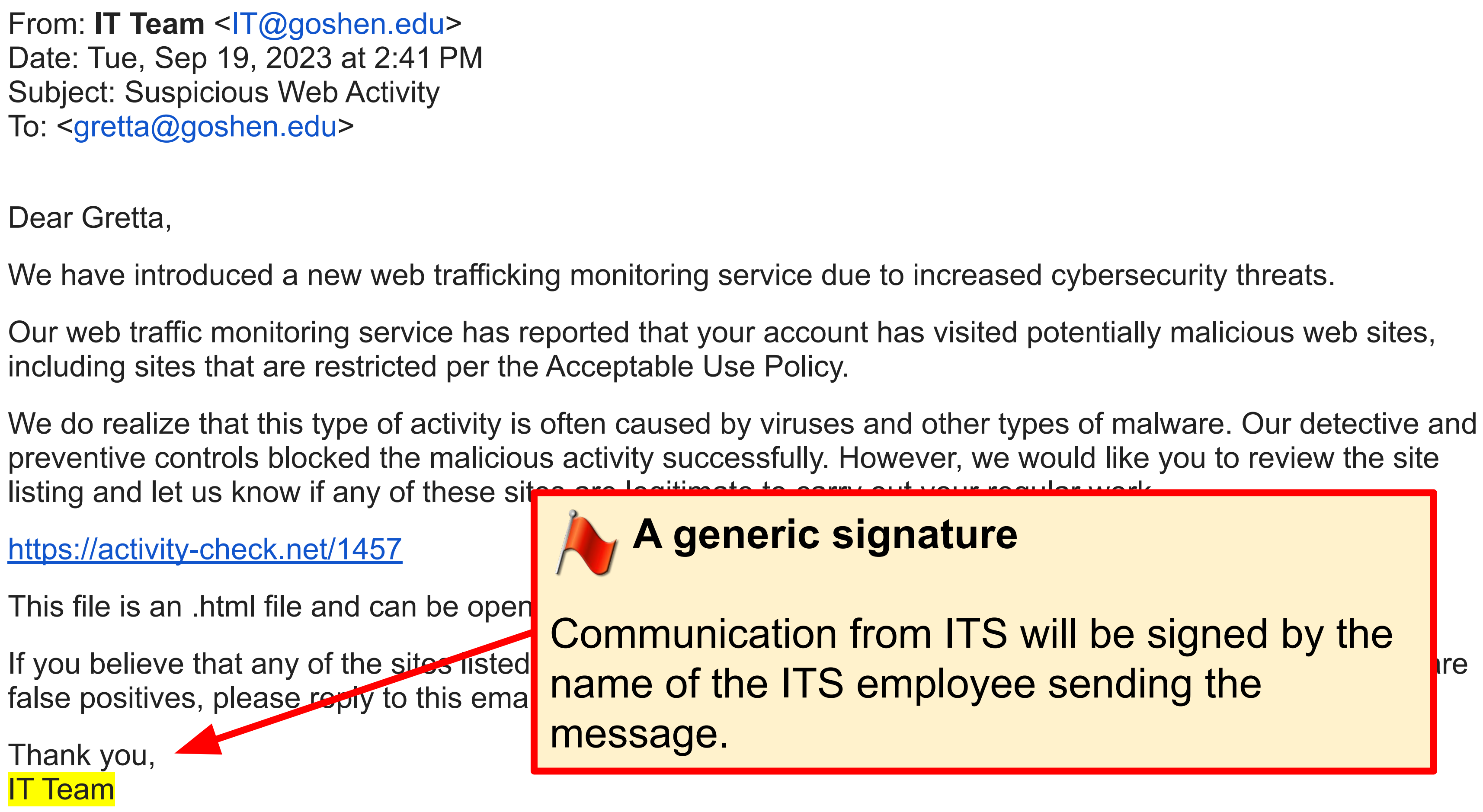
We do realize that this type of activity is often caused by viruses and other types of malware. Our detective and preventive controls blocked the malicious activity successfully. However, we would like you to review the site listing and let us know if any of these sites are legitimate to carry out your regular work.

https://activity-check.net/1457

This file is an .html file and can be opened with Google Chrome, Microsoft Edge, or Internet Explorer.

If you believe that any of the sites listed in the report have been reported erroneously or that all sites noted are false positives, please reply to this email.

Thank you,
IT Team



From: **IT Team** <IT@goshen.edu>
Date: Tue, Sep 19, 2023 at 2:41 PM
Subject: Suspicious Web Activity
To: <gretta@goshen.edu>

Dear Gretta,

We have introduced a new web trafficking monitoring service due to increased cybersecurity threats.

Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per the Acceptable Use Policy.

We do realize that this type of activity is often caused by viruses and other types of malware. Our detective and preventive controls blocked the malicious activity successfully. However, we would like you to review the site listing and let us know if any of these sites are legitimate to carry out your regular work.

https://activity-check.net/1457

This file is an .html file and can be open

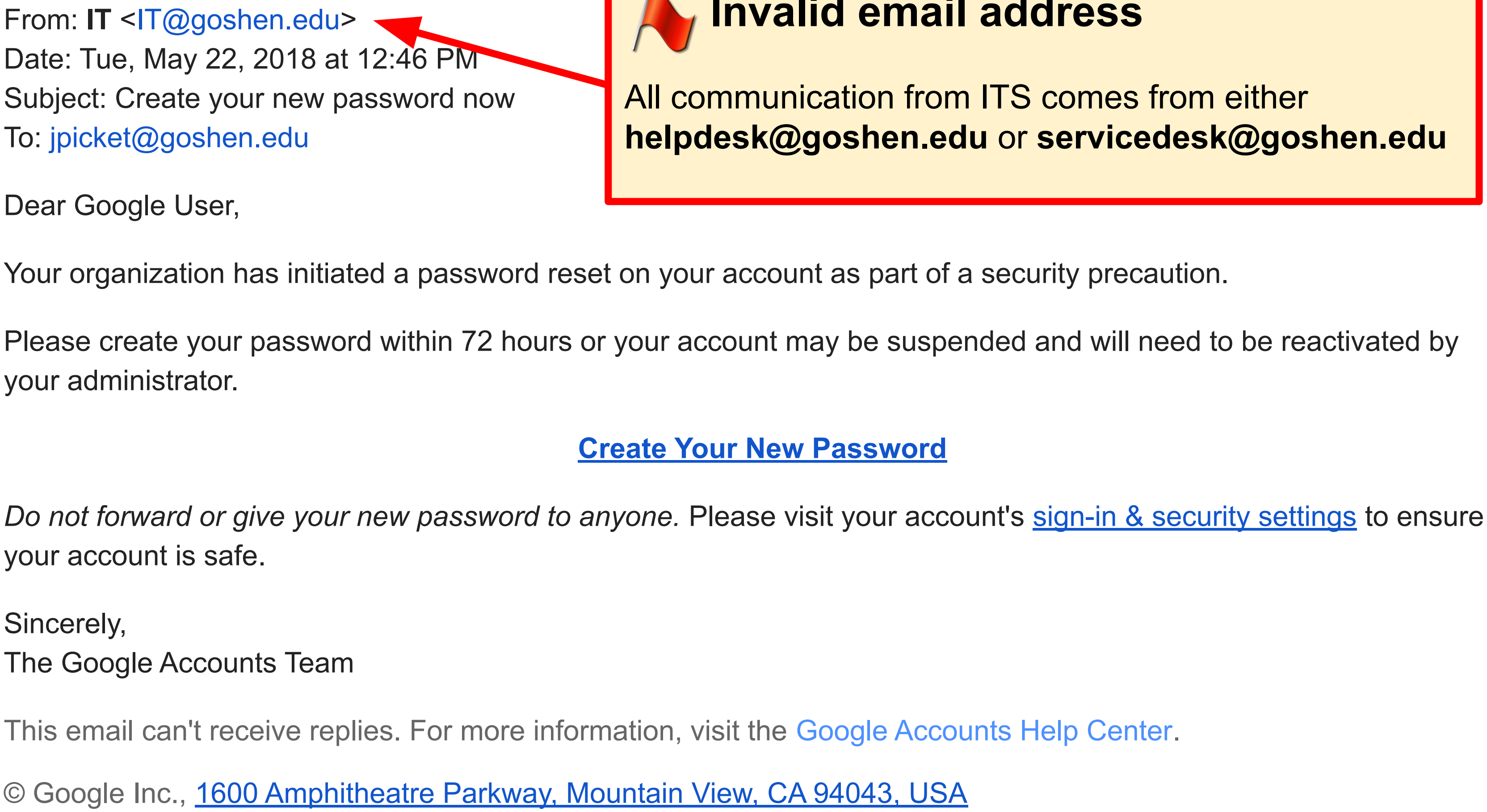
If you believe that any of the sites listed are
false positives, please reply to this ema

Thank you,
IT Team

A generic signature

Communication from ITS will be signed by the name of the ITS employee sending the message.

Phishing Example #2



From: **IT** <IT@goshen.edu>
Date: Tue, May 22, 2018 at 12:46 PM
Subject: Create your new password now
To: jpicket@goshen.edu

Invalid email address

All communication from ITS comes from either **helpdesk@goshen.edu** or **servicedesk@goshen.edu**

Dear Google User,

Your organization has initiated a password reset on your account as part of a security precaution.

Please create your password within 72 hours or your account may be suspended and will need to be reactivated by your administrator.

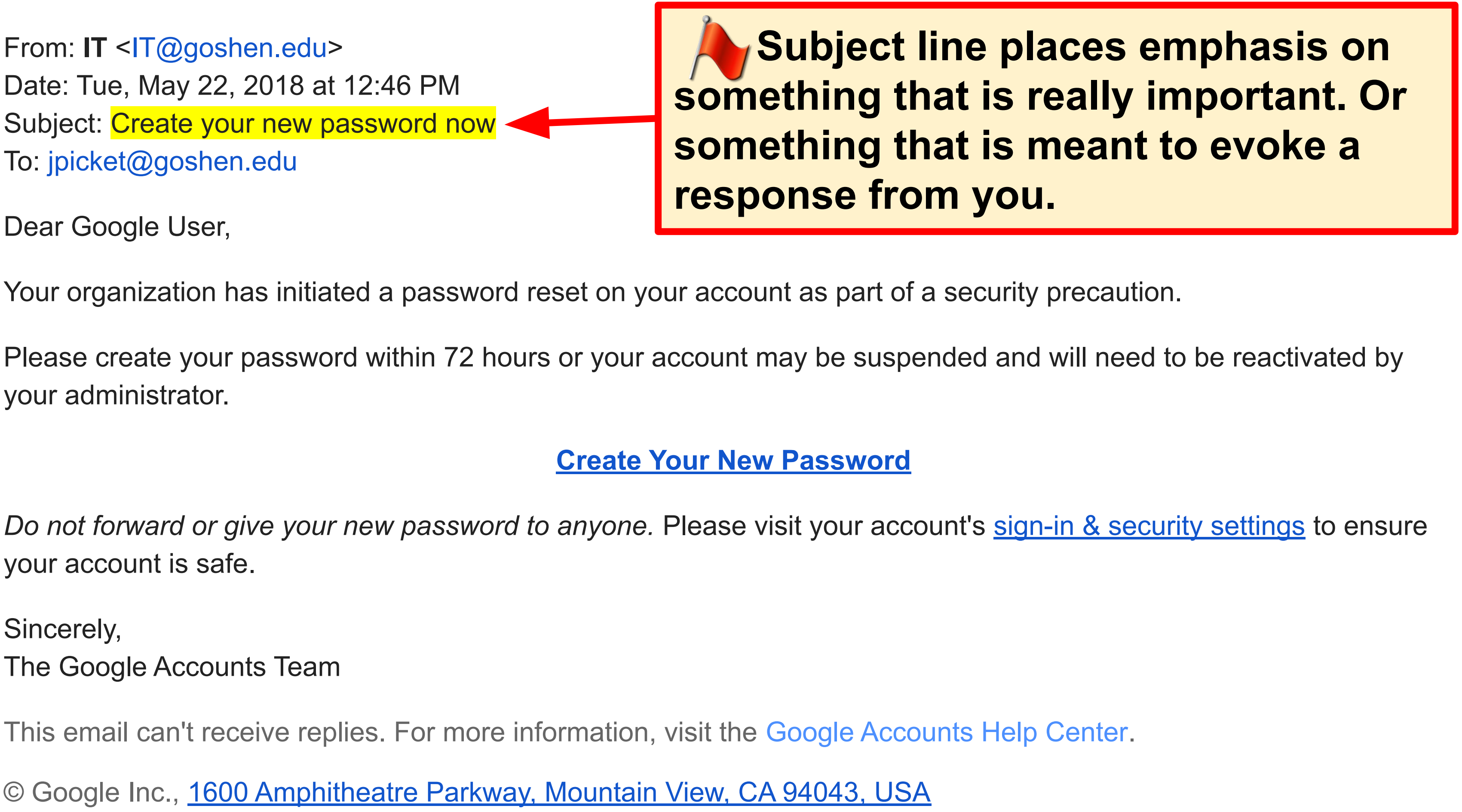
Create Your New Password

Do not forward or give your new password to anyone. Please visit your account's sign-in & security settings to ensure your account is safe.

Sincerely,
The Google Accounts Team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

© Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA



From: **IT** <IT@goshen.edu>
Date: Tue, May 22, 2018 at 12:46 PM
Subject: Create your new password now
To: jpicket@goshen.edu

Dear Google User,

Your organization has initiated a password reset on your account as part of a security precaution.

Please create your password within 72 hours or your account may be suspended and will need to be reactivated by your administrator.

Create Your New Password

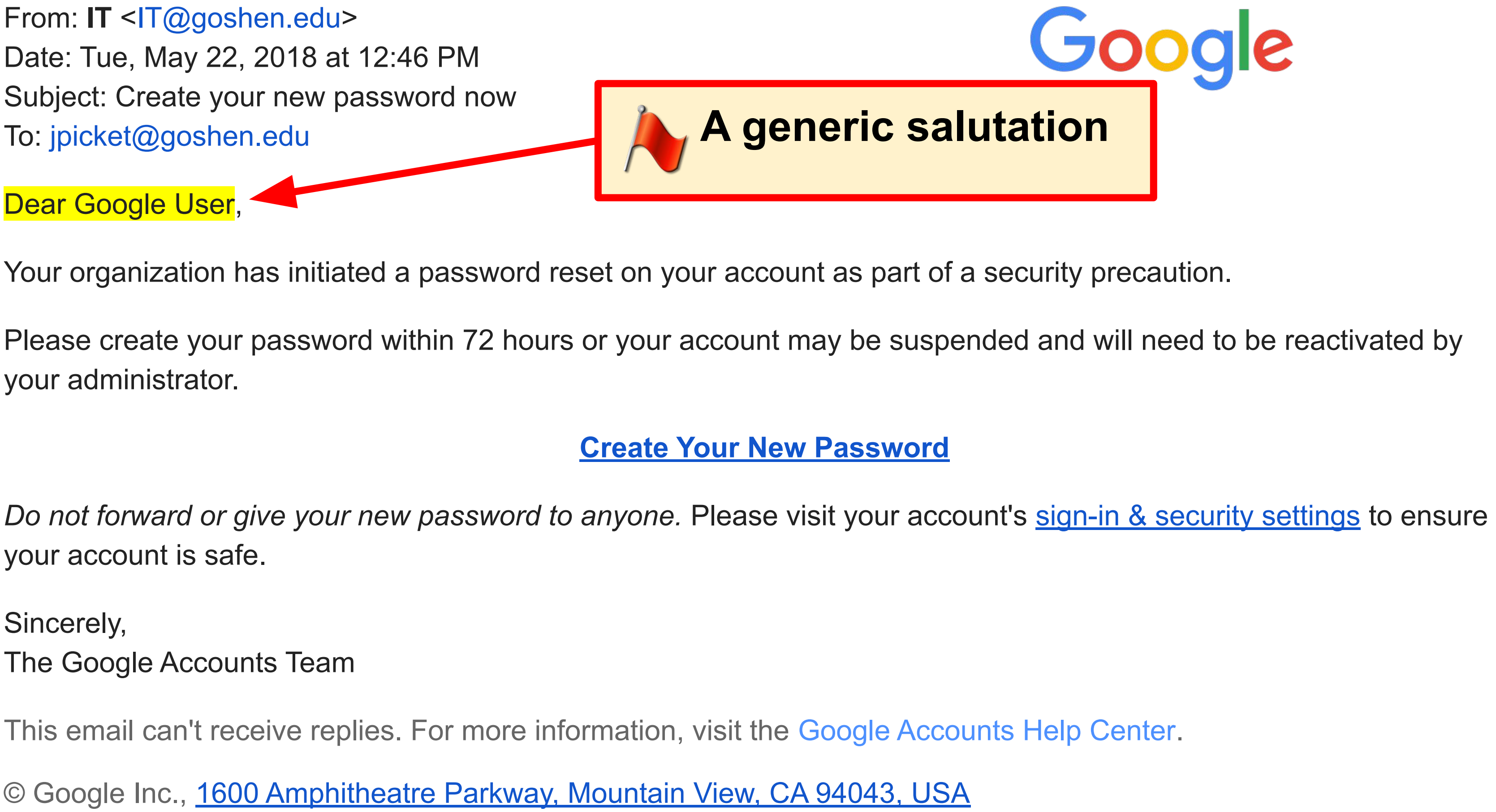
Do not forward or give your new password to anyone. Please visit your account's sign-in & security settings to ensure your account is safe.

Sincerely,
The Google Accounts Team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

© Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

🚩 **Subject line places emphasis on something that is really important. Or something that is meant to evoke a response from you.**



From: **IT** <IT@goshen.edu>
Date: Tue, May 22, 2018 at 12:46 PM
Subject: Create your new password now
To: jpicket@goshen.edu

Dear Google User,

Your organization has initiated a password reset on your account as part of a security precaution.

Please create your password within 72 hours or your account may be suspended and will need to be reactivated by your administrator.

Create Your New Password

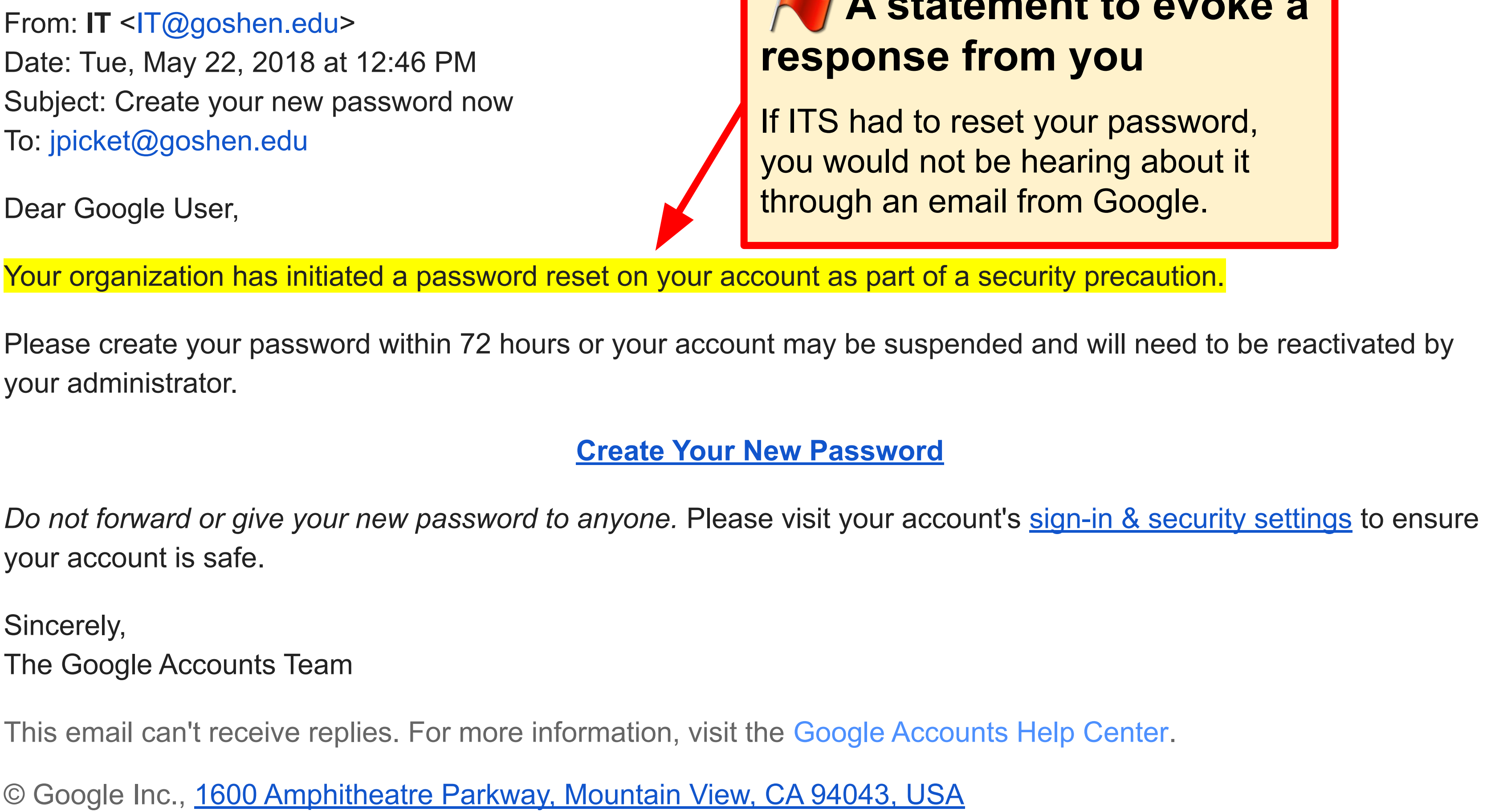
Do not forward or give your new password to anyone. Please visit your account's sign-in & security settings to ensure your account is safe.

Sincerely,
The Google Accounts Team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

© Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

A generic salutation



From: **IT** <IT@goshen.edu>
Date: Tue, May 22, 2018 at 12:46 PM
Subject: Create your new password now
To: jpicket@goshen.edu

Dear Google User,

Your organization has initiated a password reset on your account as part of a security precaution.

Please create your password within 72 hours or your account may be suspended and will need to be reactivated by your administrator.

Create Your New Password

Do not forward or give your new password to anyone. Please visit your account's sign-in & security settings to ensure your account is safe.

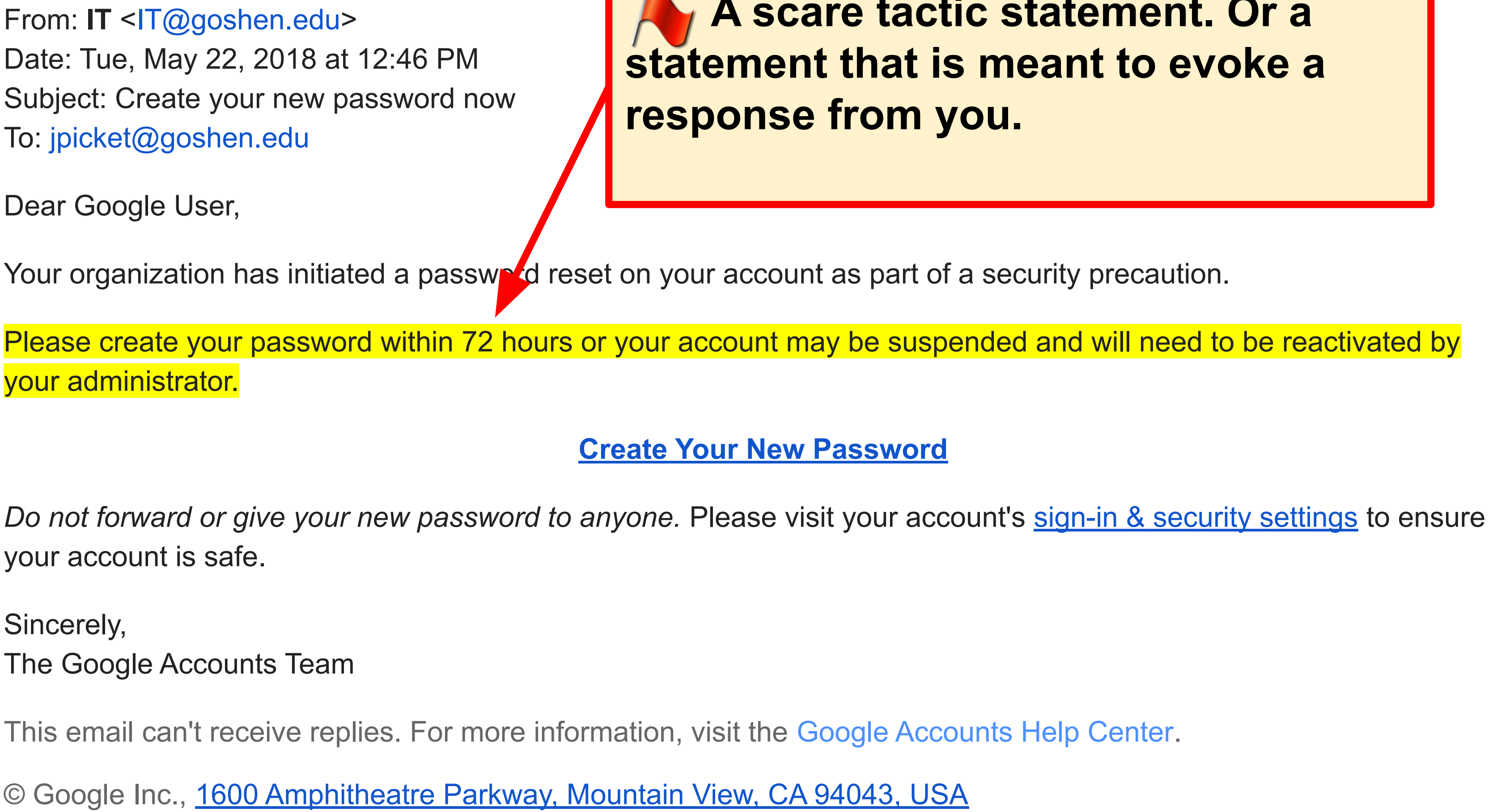
Sincerely,
The Google Accounts Team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

© Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

A statement to evoke a response from you

If ITS had to reset your password, you would not be hearing about it through an email from Google.



From: **IT** <IT@goshen.edu>
Date: Tue, May 22, 2018 at 12:46 PM
Subject: Create your new password now
To: jpicket@goshen.edu

Dear Google User,

Your organization has initiated a password reset on your account as part of a security precaution.

Please create your password within 72 hours or your account may be suspended and will need to be reactivated by your administrator.

Create Your New Password

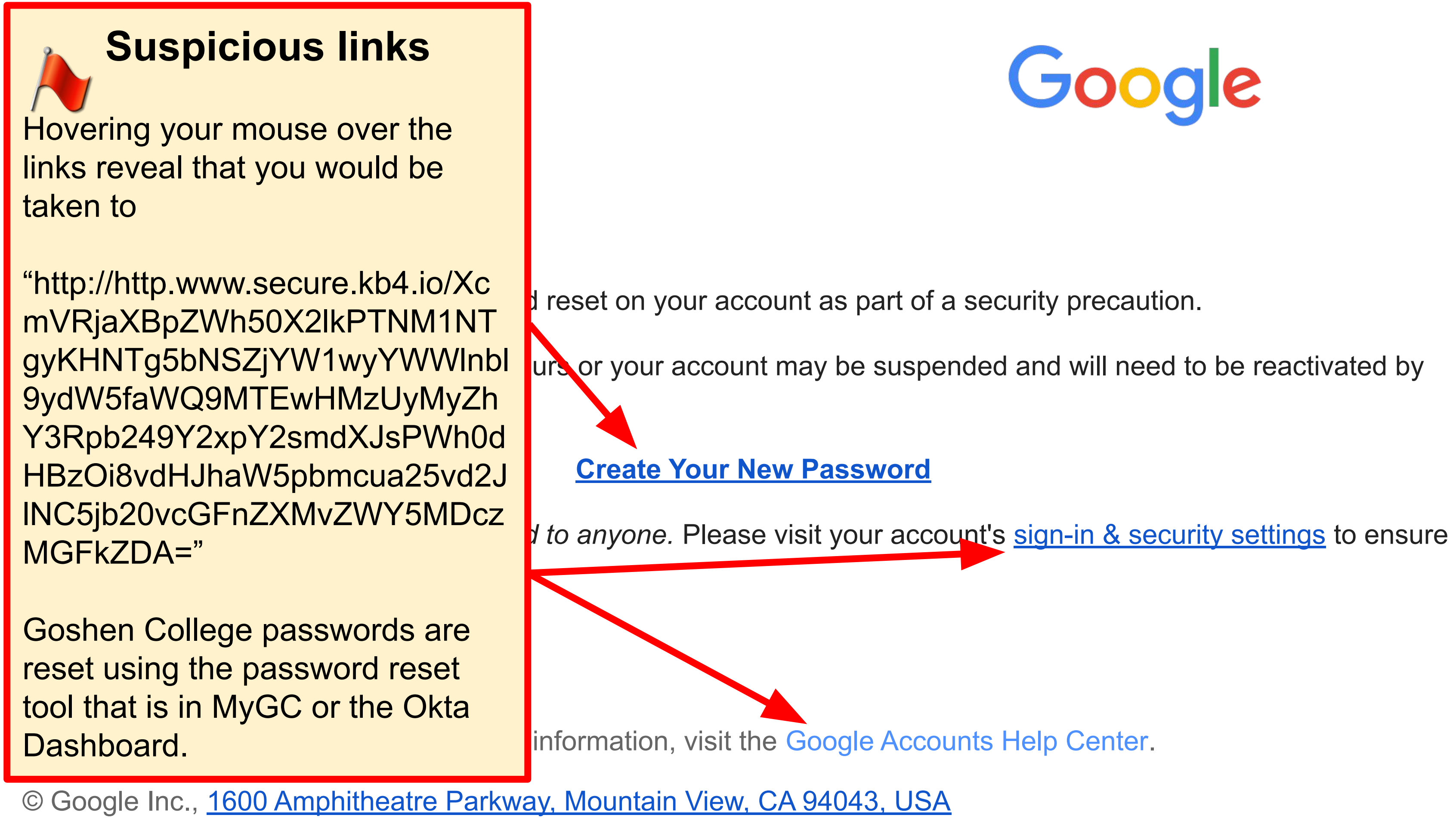
Do not forward or give your new password to anyone. Please visit your account's sign-in & security settings to ensure your account is safe.

Sincerely,
The Google Accounts Team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

© Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

A scare tactic statement. Or a statement that is meant to evoke a response from you.



Suspicious links

Hovering your mouse over the links reveal that you would be taken to

“http://http.www.secure.kb4.io/XcmVRjaXBpZWh50X2lkPTNM1NTgyKHNTg5bNSZjYW1wyYWWlnbl9ydW5faWQ9MTEwHMzUyMyZhY3Rpb249Y2xpY2smdXJsPWh0dHBzOi8vdHJhaW5pbmcua25vd2JlNC5jb20vcGFnZXMvZWY5MDczMGFkZDA=”

Goshen College passwords are reset using the password reset tool that is in MyGC or the Okta Dashboard.

d reset on your account as part of a security precaution.

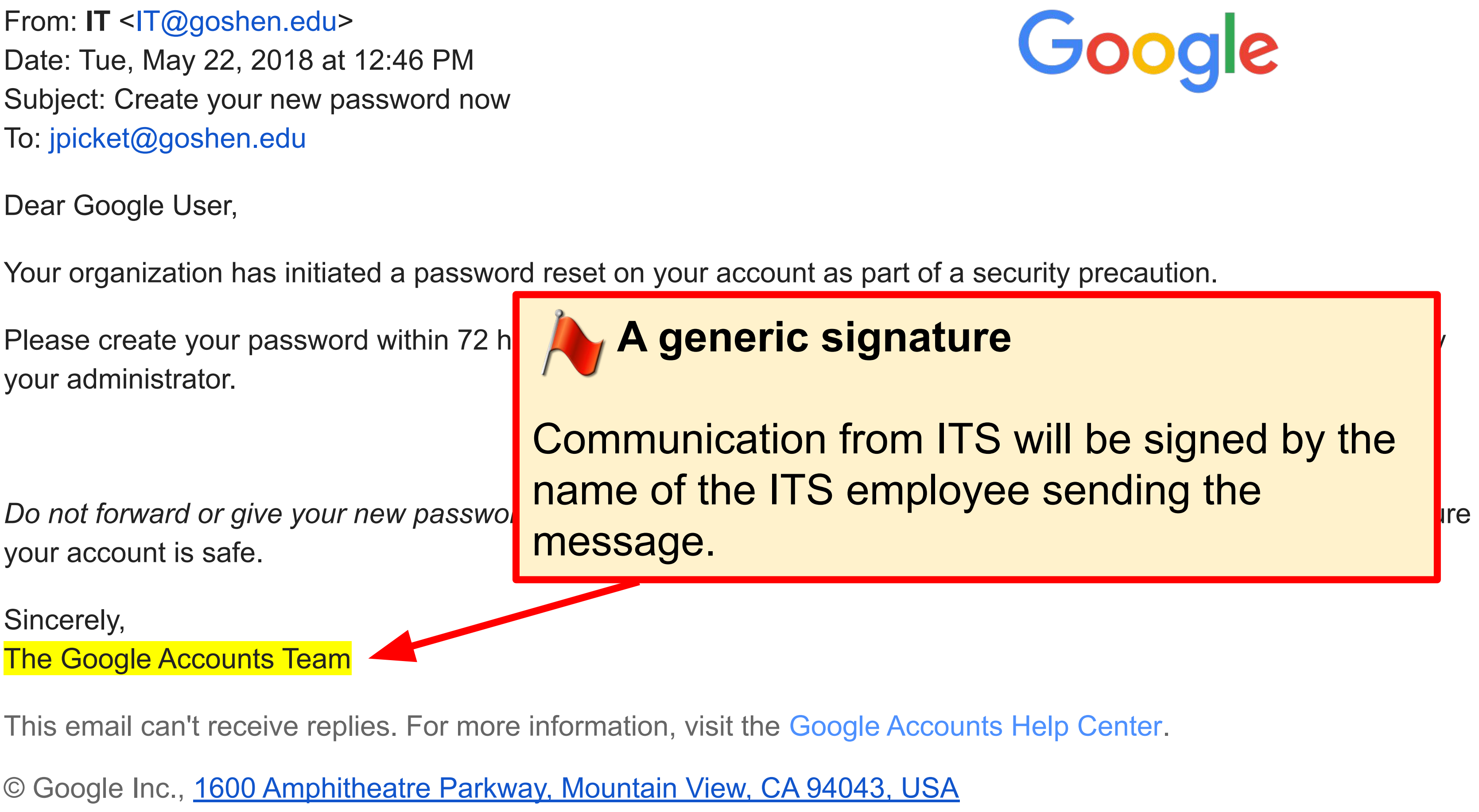
urs or your account may be suspended and will need to be reactivated by

Create Your New Password

d to anyone. Please visit your account's sign-in & security settings to ensure

information, visit the Google Accounts Help Center.

© Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA



From: **IT** <IT@goshen.edu>
Date: Tue, May 22, 2018 at 12:46 PM
Subject: Create your new password now
To: jpicket@goshen.edu

Dear Google User,

Your organization has initiated a password reset on your account as part of a security precaution.

Please create your password within 72 h y
your administrator.

Do not forward or give your new passwo ure
your account is safe.

Sincerely,
The Google Accounts Team

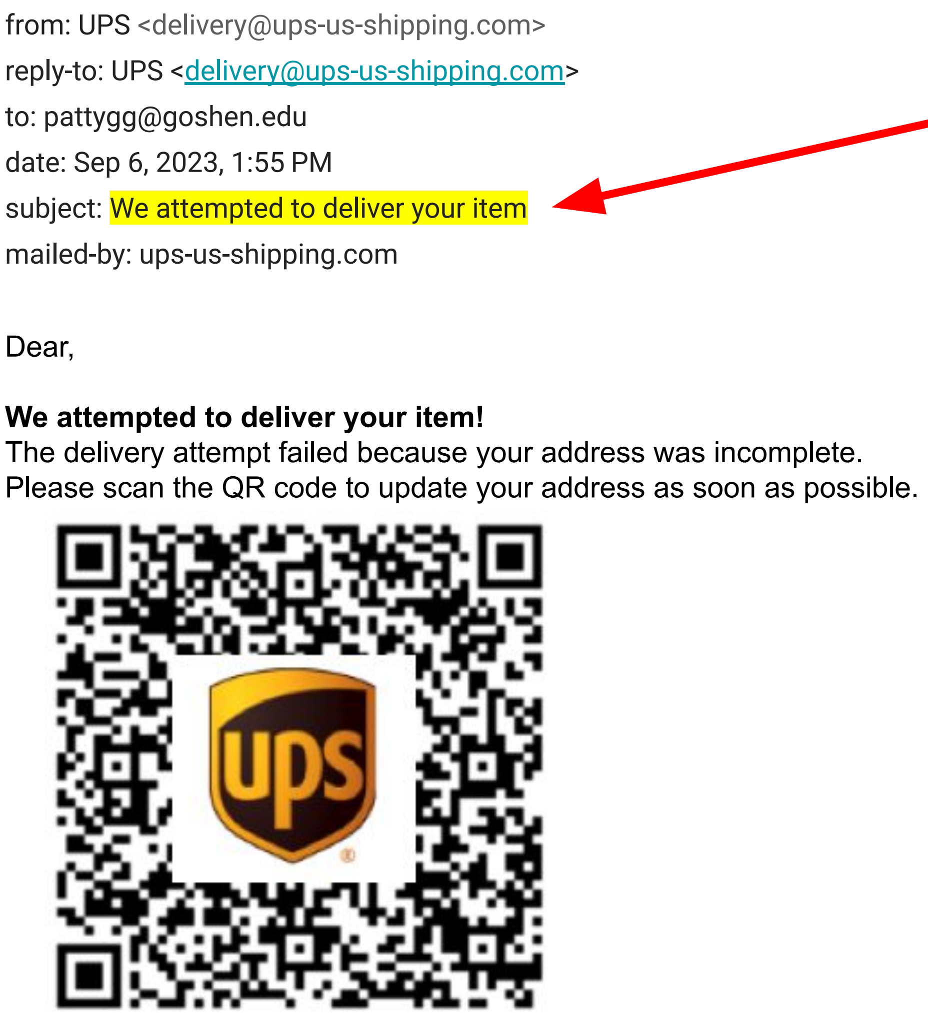
This email can't receive replies. For more information, visit the Google Accounts Help Center.

© Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

A generic signature

Communication from ITS will be signed by the name of the ITS employee sending the message.

Phishing Example #3

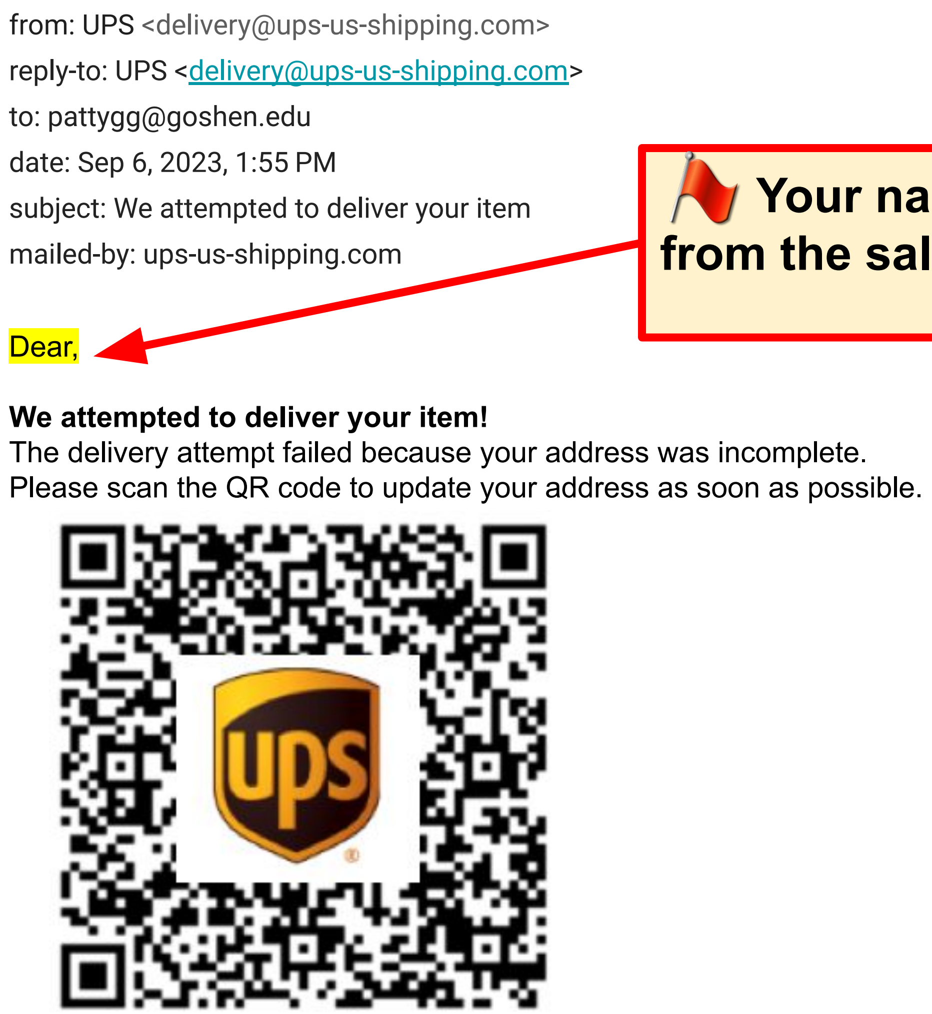


from: UPS <delivery@ups-us-shipping.com>
reply-to: UPS <delivery@ups-us-shipping.com>
to: pattygg@goshen.edu
date: Sep 6, 2023, 1:55 PM
subject: We attempted to deliver your item
mailed-by: ups-us-shipping.com

Dear,

We attempted to deliver your item!
The delivery attempt failed because your address was incomplete.
Please scan the QR code to update your address as soon as possible.

🚩 **Are you expecting a package from UPS?**



from: UPS <delivery@ups-us-shipping.com>

reply-to: UPS <delivery@ups-us-shipping.com>

to: pattygg@goshen.edu

date: Sep 6, 2023, 1:55 PM

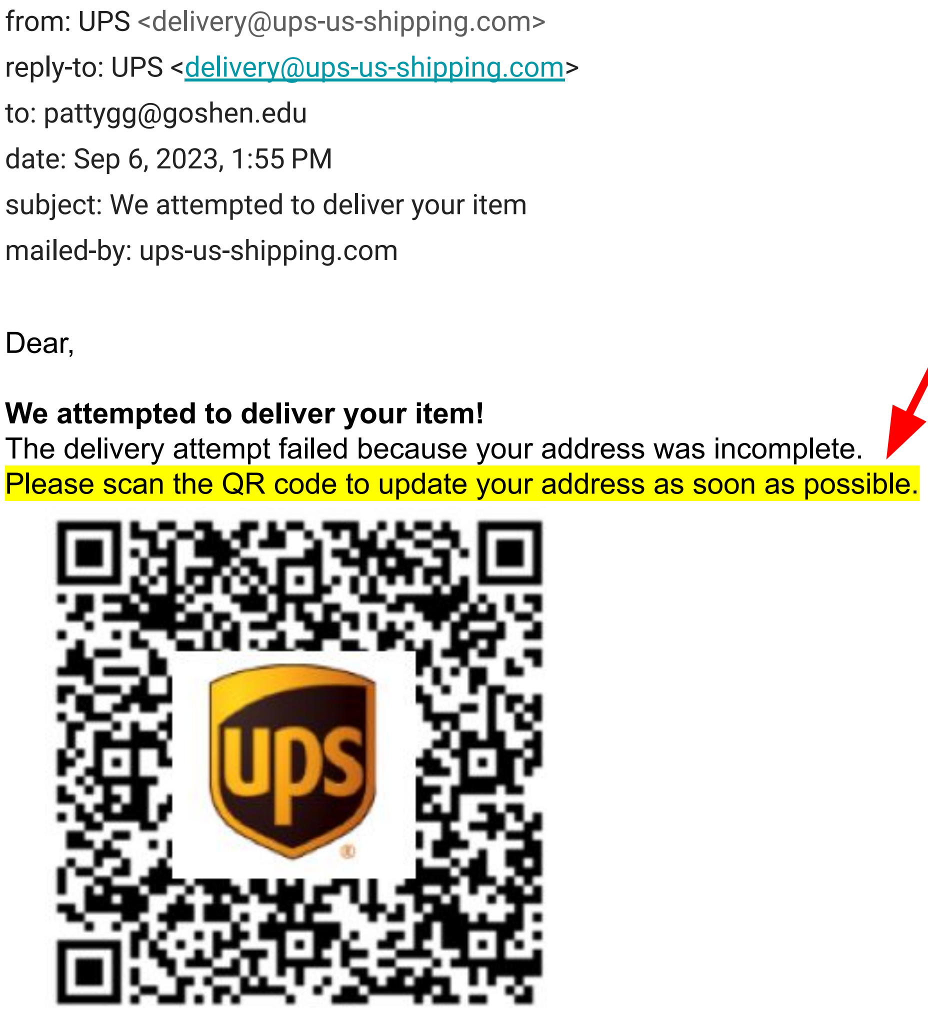
subject: We attempted to deliver your item

mailed-by: ups-us-shipping.com

Dear,

We attempted to deliver your item!
The delivery attempt failed because your address was incomplete.
Please scan the QR code to update your address as soon as possible.

🚩 **Your name is missing from the salutation**



from: UPS <delivery@ups-us-shipping.com>

reply-to: UPS <delivery@ups-us-shipping.com>

to: pattygg@goshen.edu

date: Sep 6, 2023, 1:55 PM

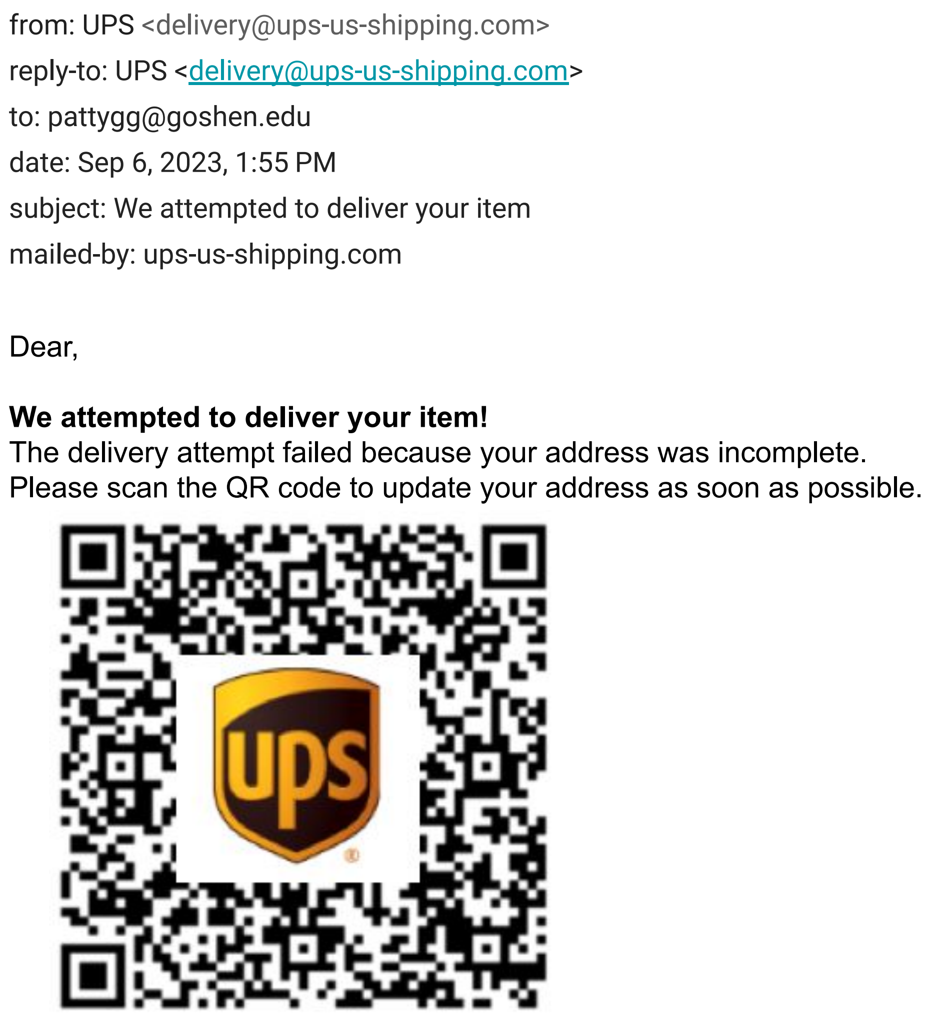
subject: We attempted to deliver your item

mailed-by: ups-us-shipping.com

Dear,

We attempted to deliver your item!
The delivery attempt failed because your address was incomplete.
Please scan the QR code to update your address as soon as possible.

🚩 **An urgent request or time sensitive action is needed**



from: UPS <delivery@ups-us-shipping.com>

reply-to: UPS <delivery@ups-us-shipping.com>

to: pattygg@goshen.edu

date: Sep 6, 2023, 1:55 PM

subject: We attempted to deliver your item

mailed-by: ups-us-shipping.com

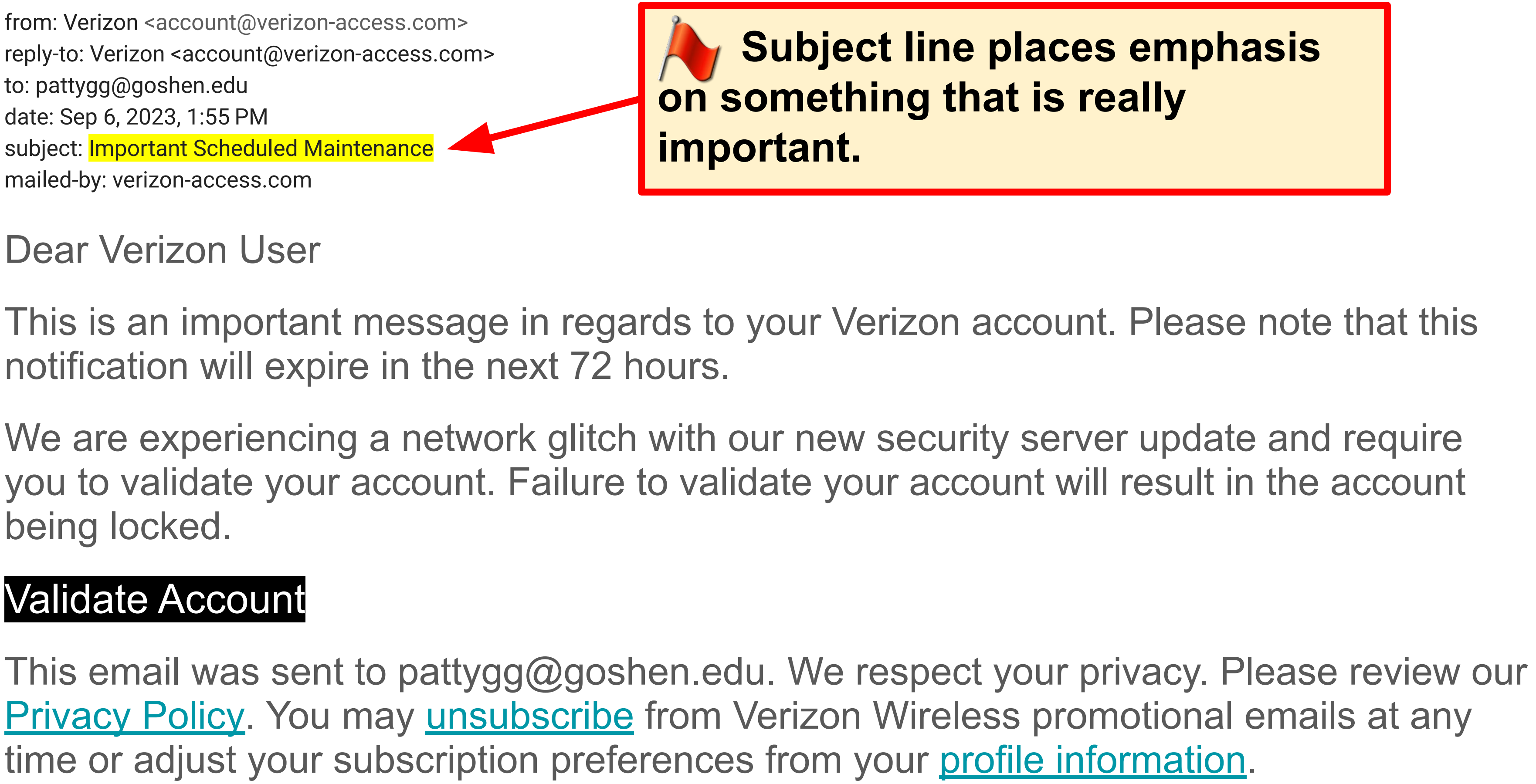
Dear,

We attempted to deliver your item!
The delivery attempt failed because your address was incomplete.
Please scan the QR code to update your address as soon as possible.

Can you trust a QR code?

Cybercriminals take advantage of the convenience that QR codes offer, and trick you into scanning without thinking. The QR code directs you to a fake website where they can capture anything that you type in.

Phishing Example #4



from: Verizon <account@verizon-access.com>
reply-to: Verizon <account@verizon-access.com>
to: pattygg@goshen.edu
date: Sep 6, 2023, 1:55 PM
subject: Important Scheduled Maintenance
mailed-by: verizon-access.com

🚩 **Subject line places emphasis on something that is really important.**

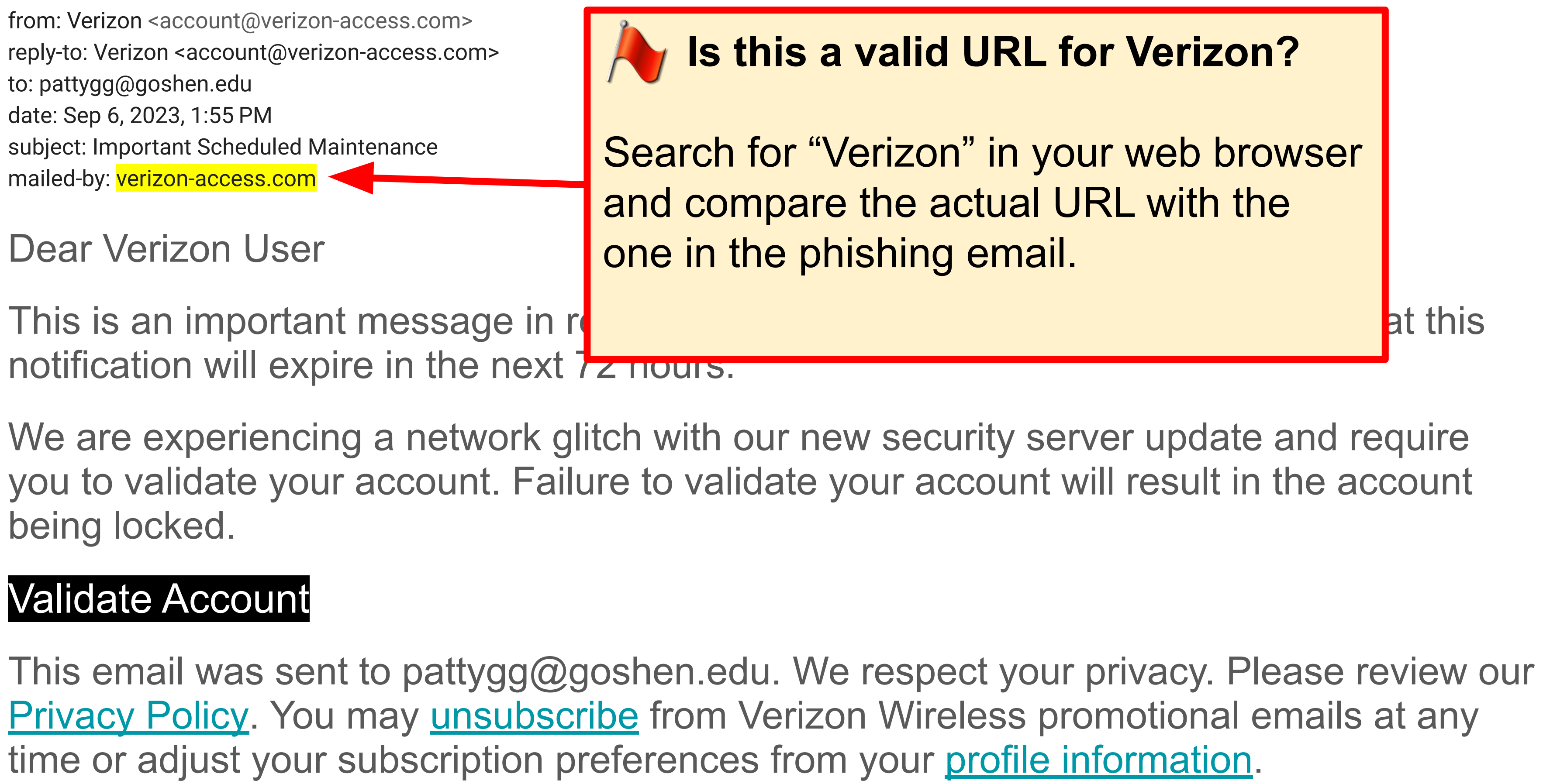
Dear Verizon User

This is an important message in regards to your Verizon account. Please note that this notification will expire in the next 72 hours.

We are experiencing a network glitch with our new security server update and require you to validate your account. Failure to validate your account will result in the account being locked.

Validate Account

This email was sent to pattygg@goshen.edu. We respect your privacy. Please review our Privacy Policy. You may unsubscribe from Verizon Wireless promotional emails at any time or adjust your subscription preferences from your profile information.



from: Verizon <account@verizon-access.com>
reply-to: Verizon <account@verizon-access.com>
to: pattygg@goshen.edu
date: Sep 6, 2023, 1:55 PM
subject: Important Scheduled Maintenance
mailed-by: verizon-access.com

🚩 Is this a valid URL for Verizon?

Search for “Verizon” in your web browser and compare the actual URL with the one in the phishing email.

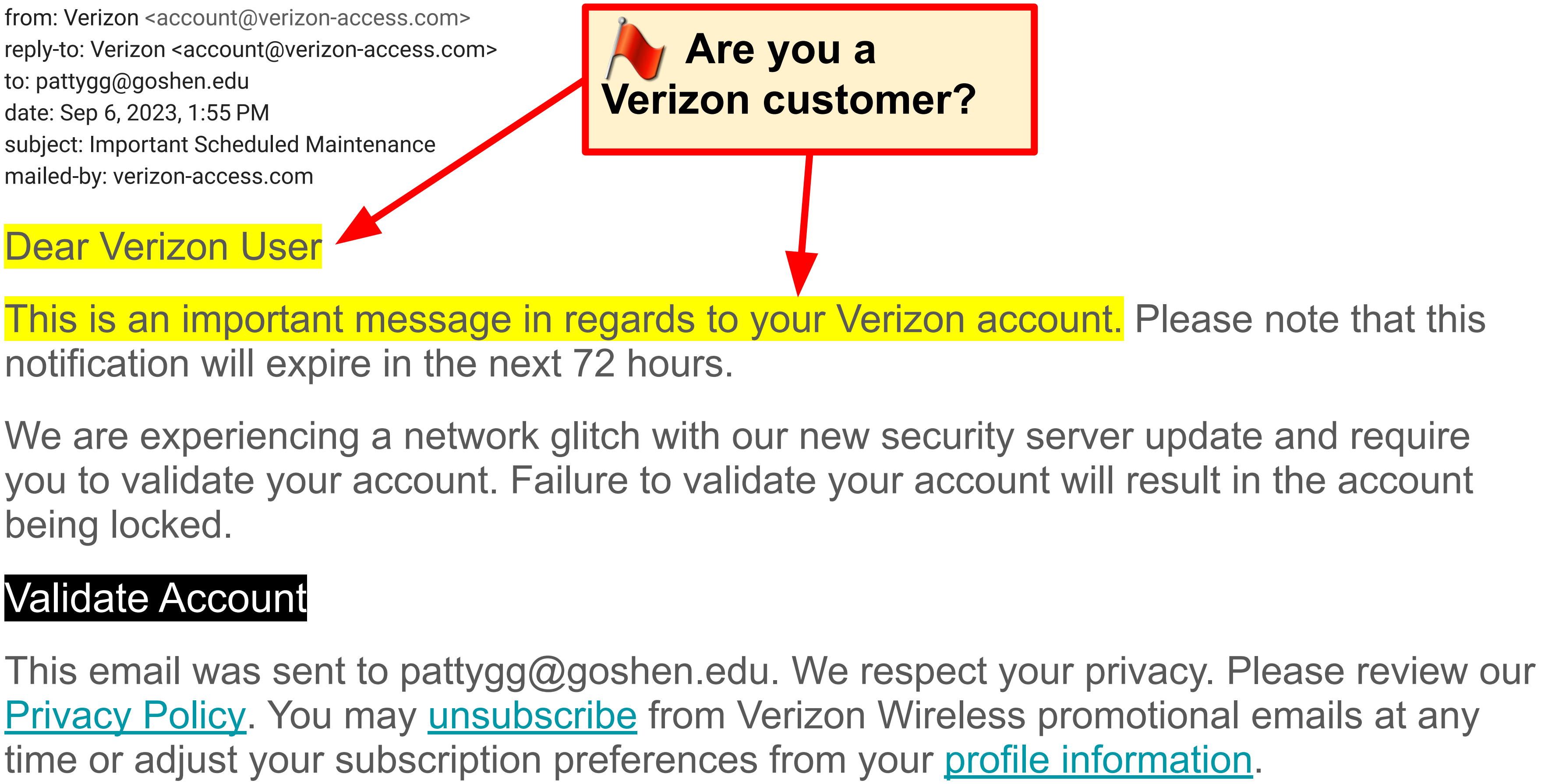
Dear Verizon User

This is an important message in r at this notification will expire in the next 72 hours.

We are experiencing a network glitch with our new security server update and require you to validate your account. Failure to validate your account will result in the account being locked.

Validate Account

This email was sent to pattygg@goshen.edu. We respect your privacy. Please review our Privacy Policy. You may unsubscribe from Verizon Wireless promotional emails at any time or adjust your subscription preferences from your profile information.



from: Verizon <account@verizon-access.com>
reply-to: Verizon <account@verizon-access.com>
to: pattygg@goshen.edu
date: Sep 6, 2023, 1:55 PM
subject: Important Scheduled Maintenance
mailed-by: verizon-access.com

Are you a Verizon customer?

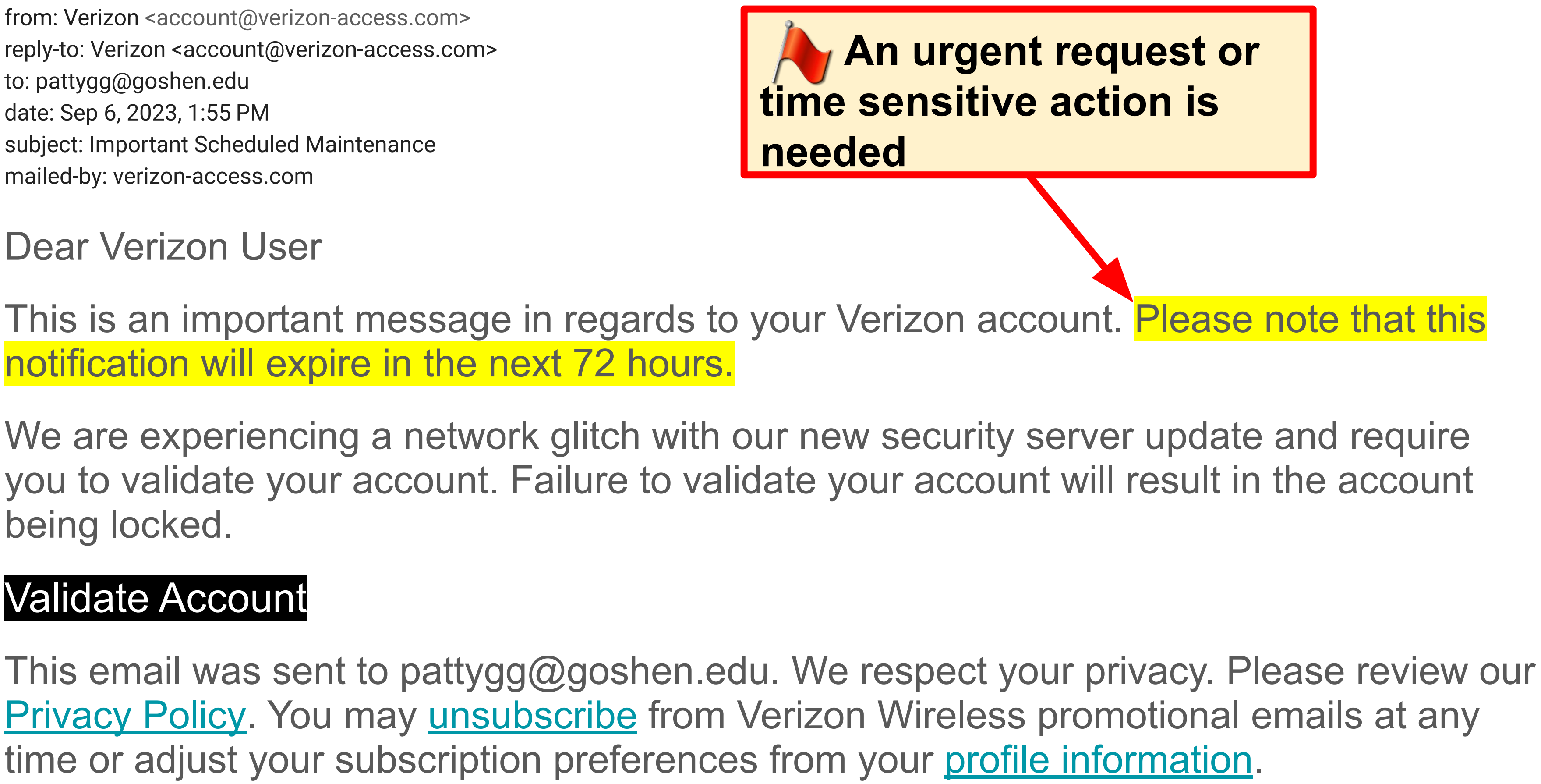
Dear Verizon User

This is an important message in regards to your Verizon account. Please note that this notification will expire in the next 72 hours.

We are experiencing a network glitch with our new security server update and require you to validate your account. Failure to validate your account will result in the account being locked.

Validate Account

This email was sent to pattygg@goshen.edu. We respect your privacy. Please review our Privacy Policy. You may unsubscribe from Verizon Wireless promotional emails at any time or adjust your subscription preferences from your profile information.



from: Verizon <account@verizon-access.com>
reply-to: Verizon <account@verizon-access.com>
to: pattygg@goshen.edu
date: Sep 6, 2023, 1:55 PM
subject: Important Scheduled Maintenance
mailed-by: verizon-access.com

🚩 **An urgent request or time sensitive action is needed**

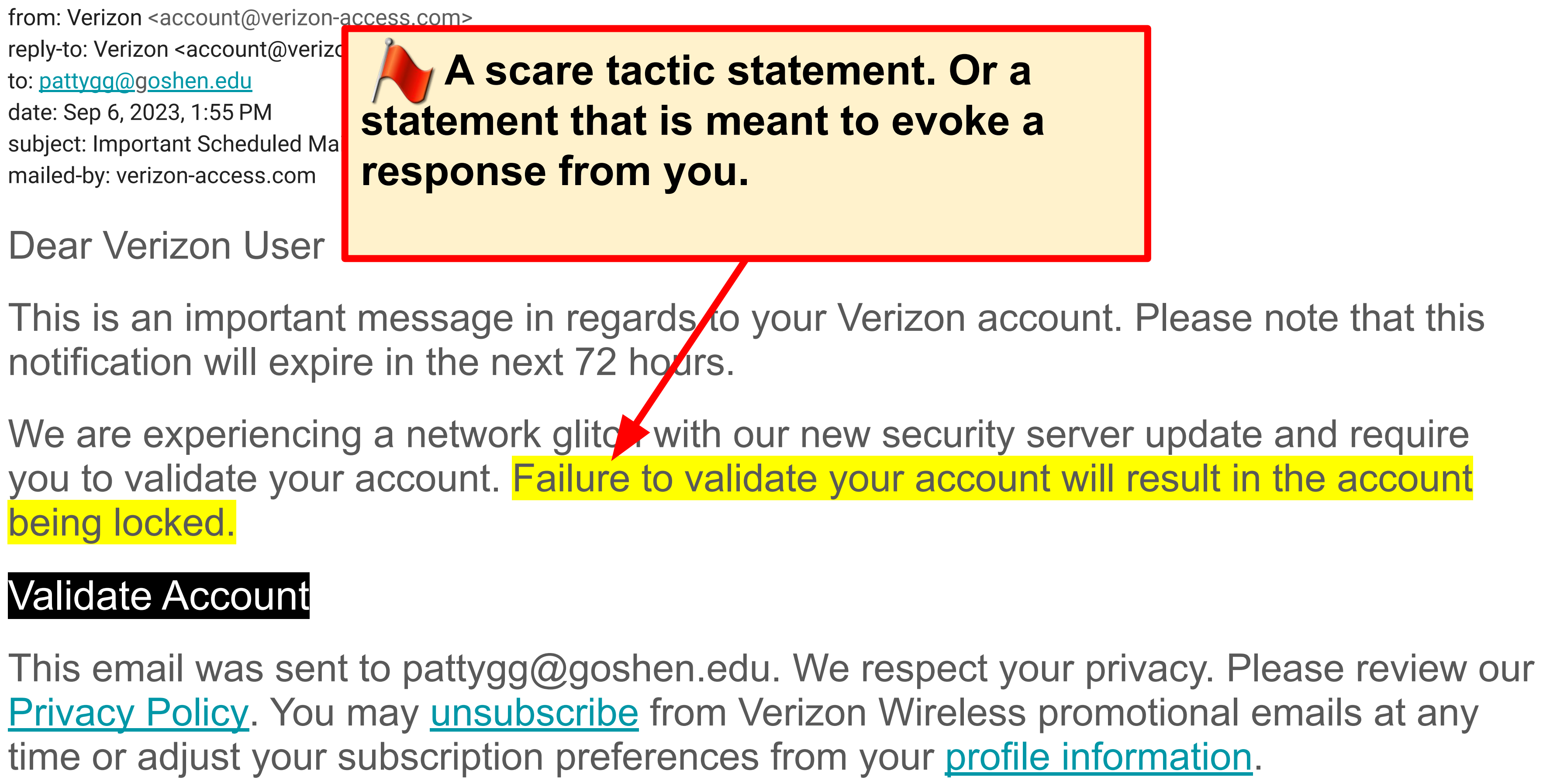
Dear Verizon User

This is an important message in regards to your Verizon account. Please note that this notification will expire in the next 72 hours.

We are experiencing a network glitch with our new security server update and require you to validate your account. Failure to validate your account will result in the account being locked.

Validate Account

This email was sent to pattygg@goshen.edu. We respect your privacy. Please review our Privacy Policy. You may unsubscribe from Verizon Wireless promotional emails at any time or adjust your subscription preferences from your profile information.



from: Verizon <account@verizon-access.com>
reply-to: Verizon <account@verizo
to: pattygg@goshen.edu
date: Sep 6, 2023, 1:55 PM
subject: Important Scheduled Ma
mailed-by: verizon-access.com

🚩 **A scare tactic statement. Or a statement that is meant to evoke a response from you.**

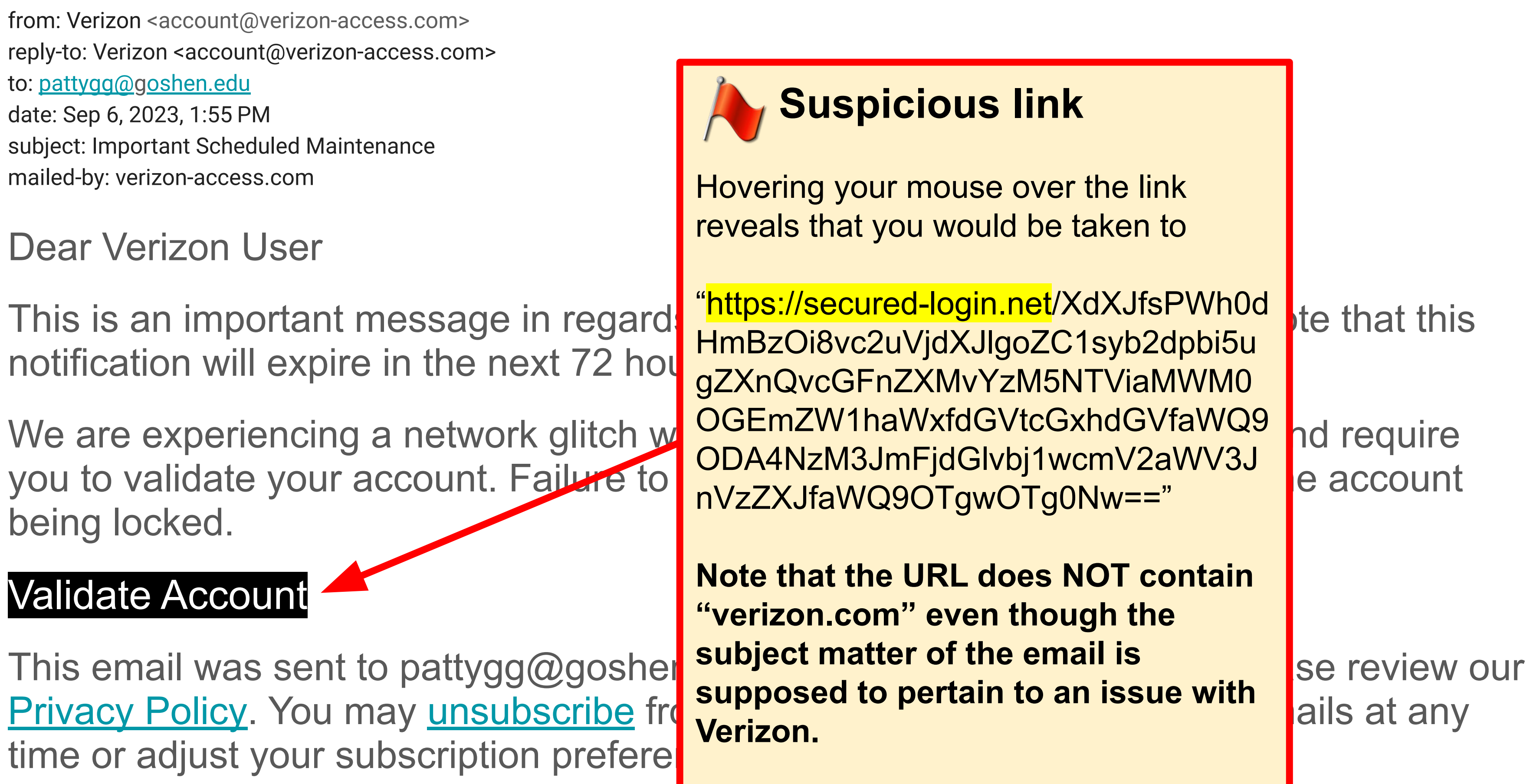
Dear Verizon User

This is an important message in regards to your Verizon account. Please note that this notification will expire in the next 72 hours.

We are experiencing a network glitch with our new security server update and require you to validate your account. Failure to validate your account will result in the account being locked.

Validate Account

This email was sent to pattygg@goshen.edu. We respect your privacy. Please review our Privacy Policy. You may unsubscribe from Verizon Wireless promotional emails at any time or adjust your subscription preferences from your profile information.



from: Verizon <account@verizon-access.com>
reply-to: Verizon <account@verizon-access.com>
to: pattygg@goshen.edu
date: Sep 6, 2023, 1:55 PM
subject: Important Scheduled Maintenance
mailed-by: verizon-access.com

Dear Verizon User

This is an important message in regards ... te that this notification will expire in the next 72 hou

We are experiencing a network glitch w ... nd require you to validate your account. Failure to ... e account being locked.

Validate Account

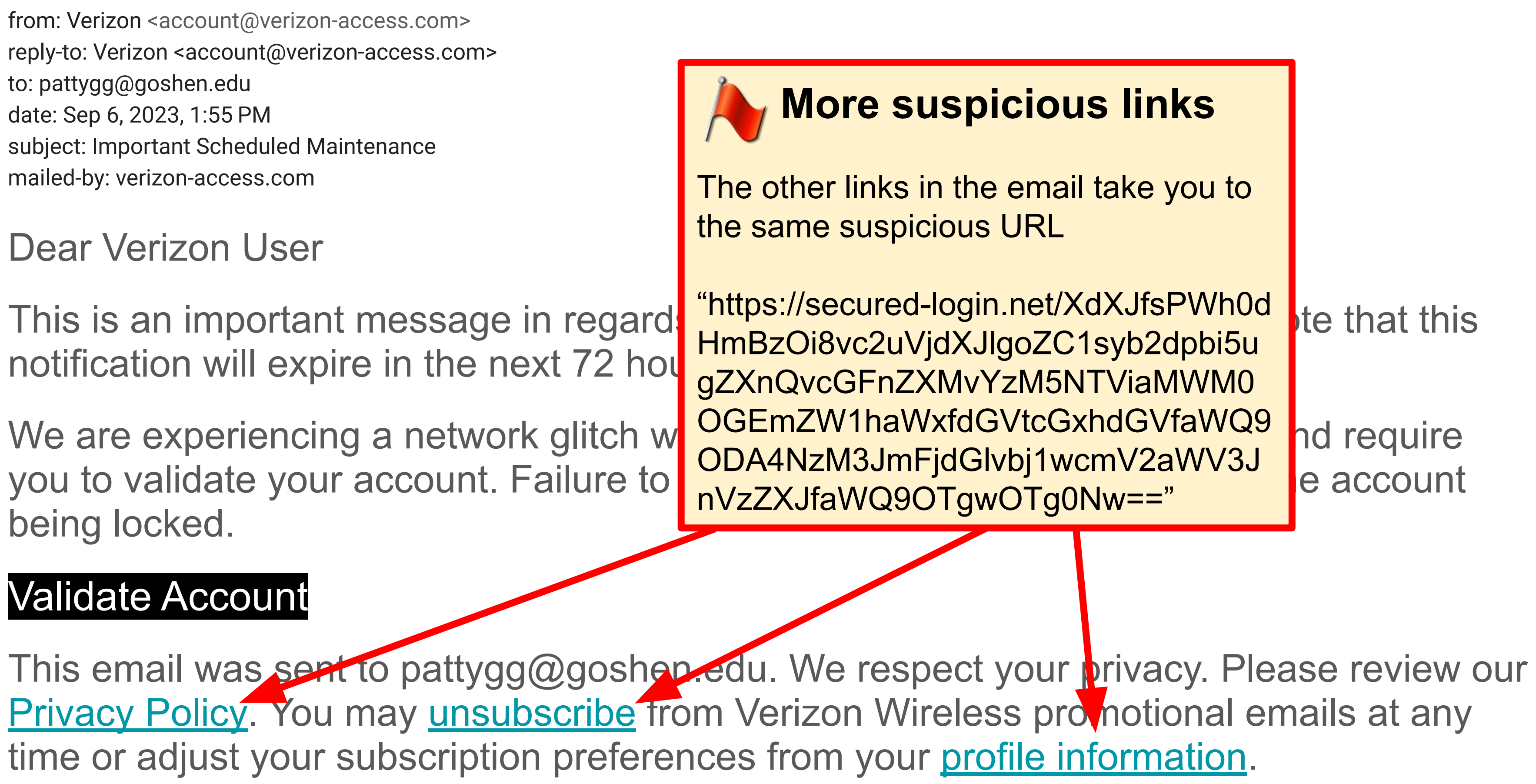
This email was sent to pattygg@goshen ... se review our Privacy Policy. You may unsubscribe fr ... ails at any time or adjust your subscription prefere

🚩 Suspicious link

Hovering your mouse over the link reveals that you would be taken to

“https://secured-login.net/XdXJfsPWh0dHmBzOi8vc2uVjdXJlgoZC1syb2dpbi5ugZXnQvcGFnZXMvYzM5NTViaMWM0OGEmZW1haWxfdGVtcGxhdGVfaWQ9ODA4NzM3JmFjdGlvbj1wcmV2aWV3JnVzZXJfaWQ9OTgwOTg0Nw==”

Note that the URL does NOT contain “verizon.com” even though the subject matter of the email is supposed to pertain to an issue with Verizon.



from: Verizon <account@verizon-access.com>
reply-to: Verizon <account@verizon-access.com>
to: pattygg@goshen.edu
date: Sep 6, 2023, 1:55 PM
subject: Important Scheduled Maintenance
mailed-by: verizon-access.com

Dear Verizon User

This is an important message in regard te that this notification will expire in the next 72 hou

We are experiencing a network glitch w nd require you to validate your account. Failure to e account being locked.

Validate Account

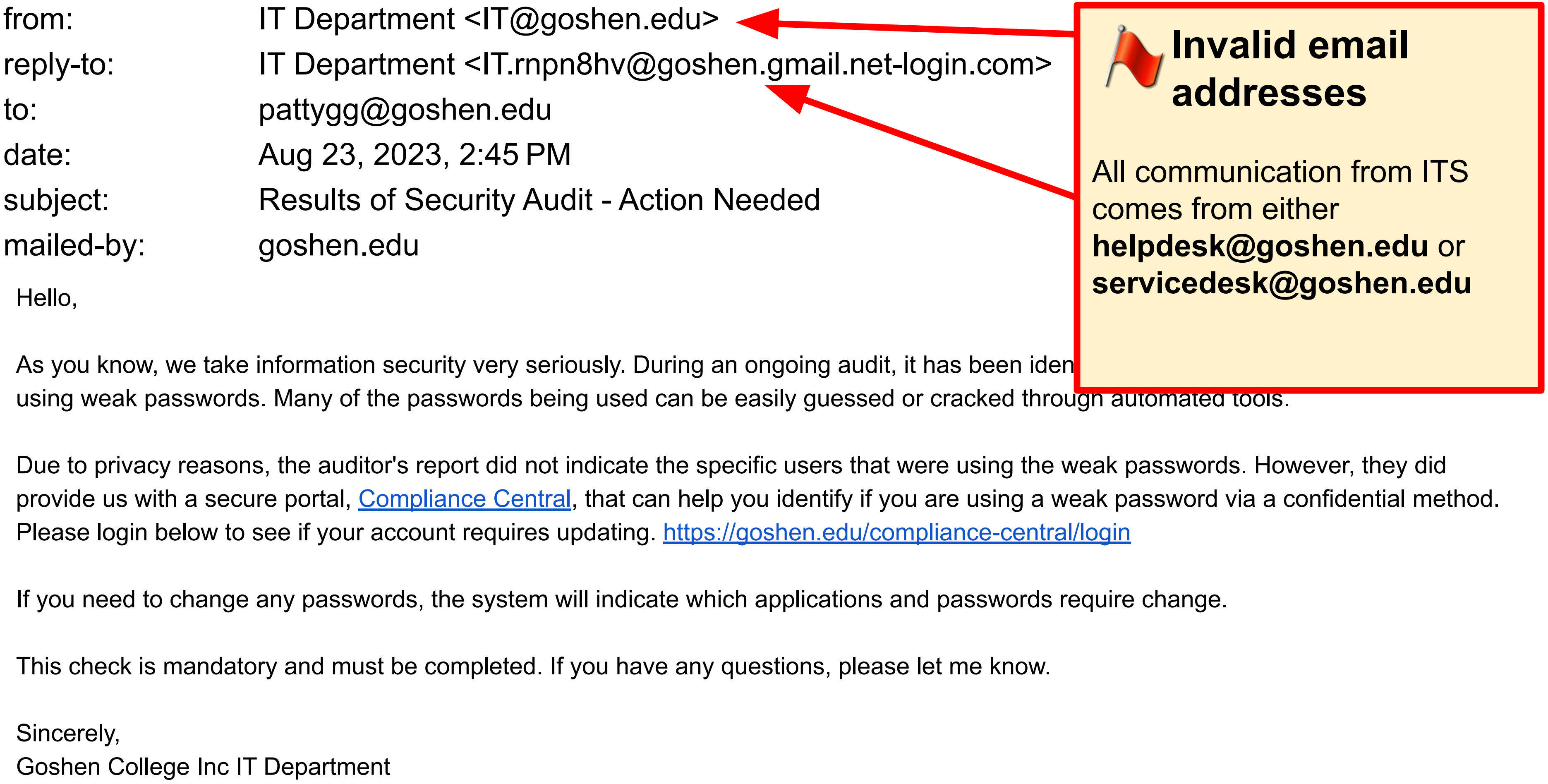
This email was sent to pattygg@goshen.edu. We respect your privacy. Please review our Privacy Policy. You may unsubscribe from Verizon Wireless promotional emails at any time or adjust your subscription preferences from your profile information.

More suspicious links

The other links in the email take you to the same suspicious URL

“https://secured-login.net/XdXJfsPWh0dHmBzOi8vc2uVjdXJlgoZC1syb2dpbi5ugZXnQvcGFnZXMvYzM5NTViaMWM0OGEmZW1haWxfdGVtcGxhdGVfaWQ9ODA4NzM3JmFjdGlvbj1wcmV2aWV3JnVzZXJfaWQ9OTgwOTg0Nw==”

Phishing Example #5



from: IT Department <IT@goshen.edu>
reply-to: IT Department <IT.rnpn8hv@goshen.gmail.net-login.com>
to: pattygg@goshen.edu
date: Aug 23, 2023, 2:45 PM
subject: Results of Security Audit - Action Needed
mailed-by: goshen.edu

Hello,

As you know, we take information security very seriously. During an ongoing audit, it has been iden using weak passwords. Many of the passwords being used can be easily guessed or cracked through automated tools.

Due to privacy reasons, the auditor's report did not indicate the specific users that were using the weak passwords. However, they did provide us with a secure portal, Compliance Central, that can help you identify if you are using a weak password via a confidential method. Please login below to see if your account requires updating. https://goshen.edu/compliance-central/login

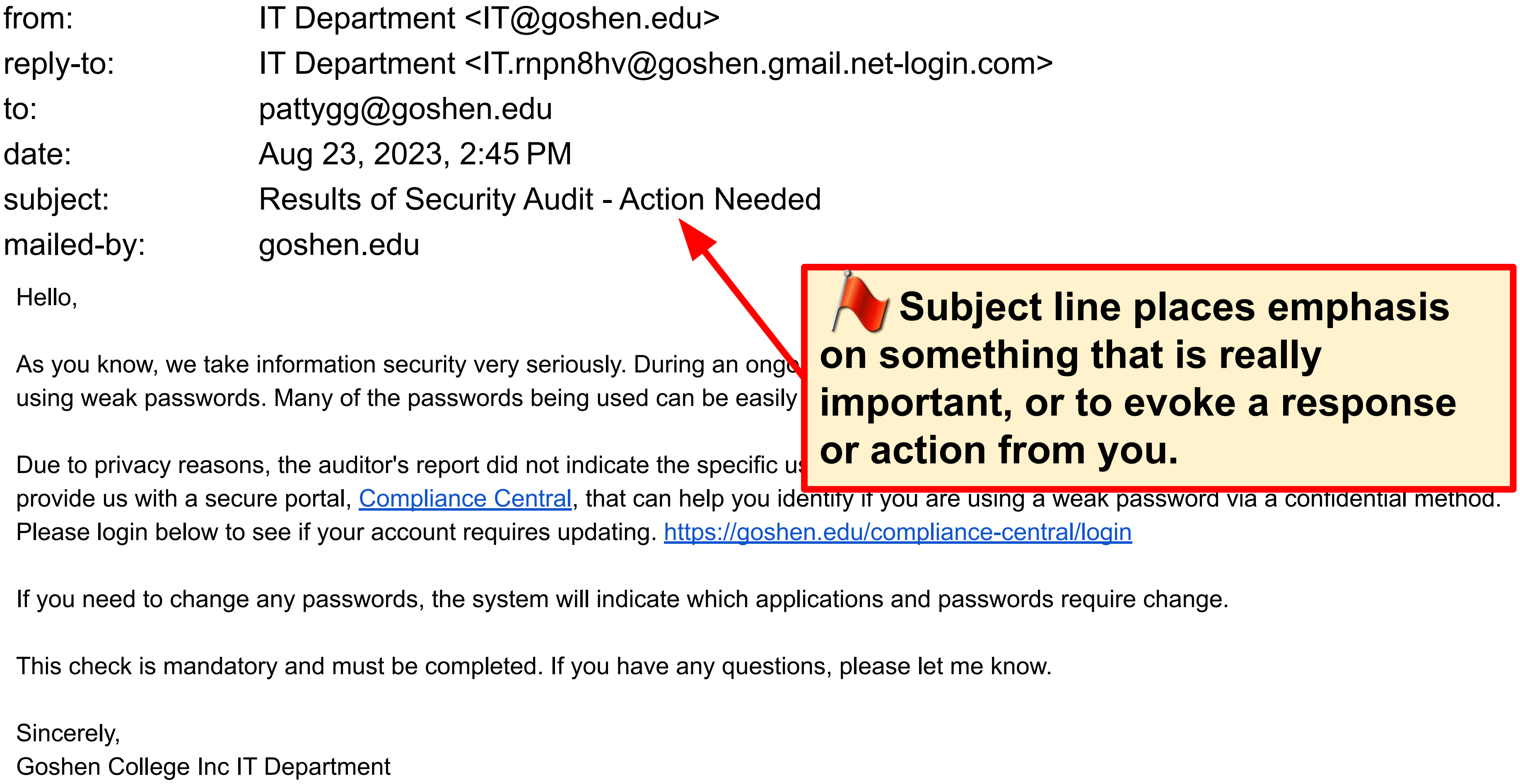
If you need to change any passwords, the system will indicate which applications and passwords require change.

This check is mandatory and must be completed. If you have any questions, please let me know.

Sincerely,
Goshen College Inc IT Department

Invalid email addresses

All communication from ITS comes from either **helpdesk@goshen.edu** or **servicedesk@goshen.edu**



from:	IT Department <IT@goshen.edu>
reply-to:	IT Department <IT.rnpn8hv@goshen.gmail.net-login.com>
to:	pattygg@goshen.edu
date:	Aug 23, 2023, 2:45 PM
subject:	Results of Security Audit - Action Needed
mailed-by:	goshen.edu

Hello,

As you know, we take information security very seriously. During an ongo
using weak passwords. Many of the passwords being used can be easily

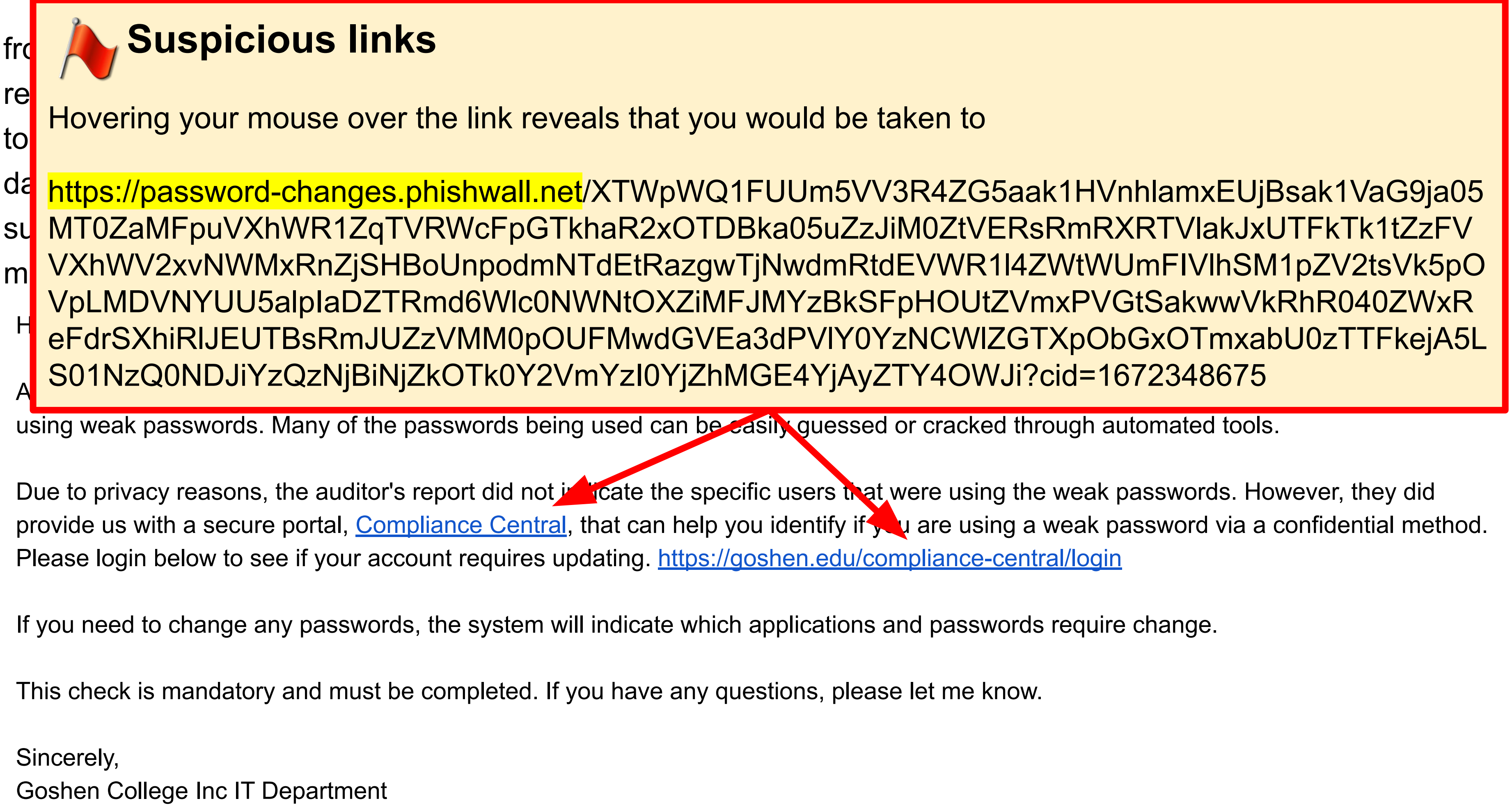
Due to privacy reasons, the auditor's report did not indicate the specific us
provide us with a secure portal, Compliance Central, that can help you identify if you are using a weak password via a confidential method. Please login below to see if your account requires updating. https://goshen.edu/compliance-central/login

If you need to change any passwords, the system will indicate which applications and passwords require change.

This check is mandatory and must be completed. If you have any questions, please let me know.

Sincerely,
Goshen College Inc IT Department

🚩 **Subject line places emphasis on something that is really important, or to evoke a response or action from you.**



Suspicious links

Hovering your mouse over the link reveals that you would be taken to

https://password-changes.phishwall.net/XTWpWQ1FUUm5VV3R4ZG5aak1HVnhlamxEUjBsak1VaG9ja05MT0ZaMFpuVXhWR1ZqTVRWcFpGTkhaR2xOTDBka05uZzJiM0ZtVERsRmRXRTVlakJxUTFkTk1tZzFVVXhWV2xvNWMxRnZjSHBoUnpodmNTdEtRazgwTjNwdmRtdEVWR1l4ZWtWUmFIVlhSM1pZV2tsVk5pOVpLMDVNYUU5alpIaDZTRmd6WlcwNWNtOXZiMFJMYzBkSFpHOUtZVmxPVGtSakwwVkRhR040ZWxReFdrSXhiRlJEUTBsRmJUZzVMM0pOUFMwdGVEa3dPVlY0YzNCWlZGTXpObGxOTmxabU0zTTFkejA5LS01NzQ0NDJiYzQzNjBiNjZkOTk0Y2VmYzI0YjZhMGE4YjAyZTY4OWJi?cid=1672348675

fro
re
to
da
su
m

H

A

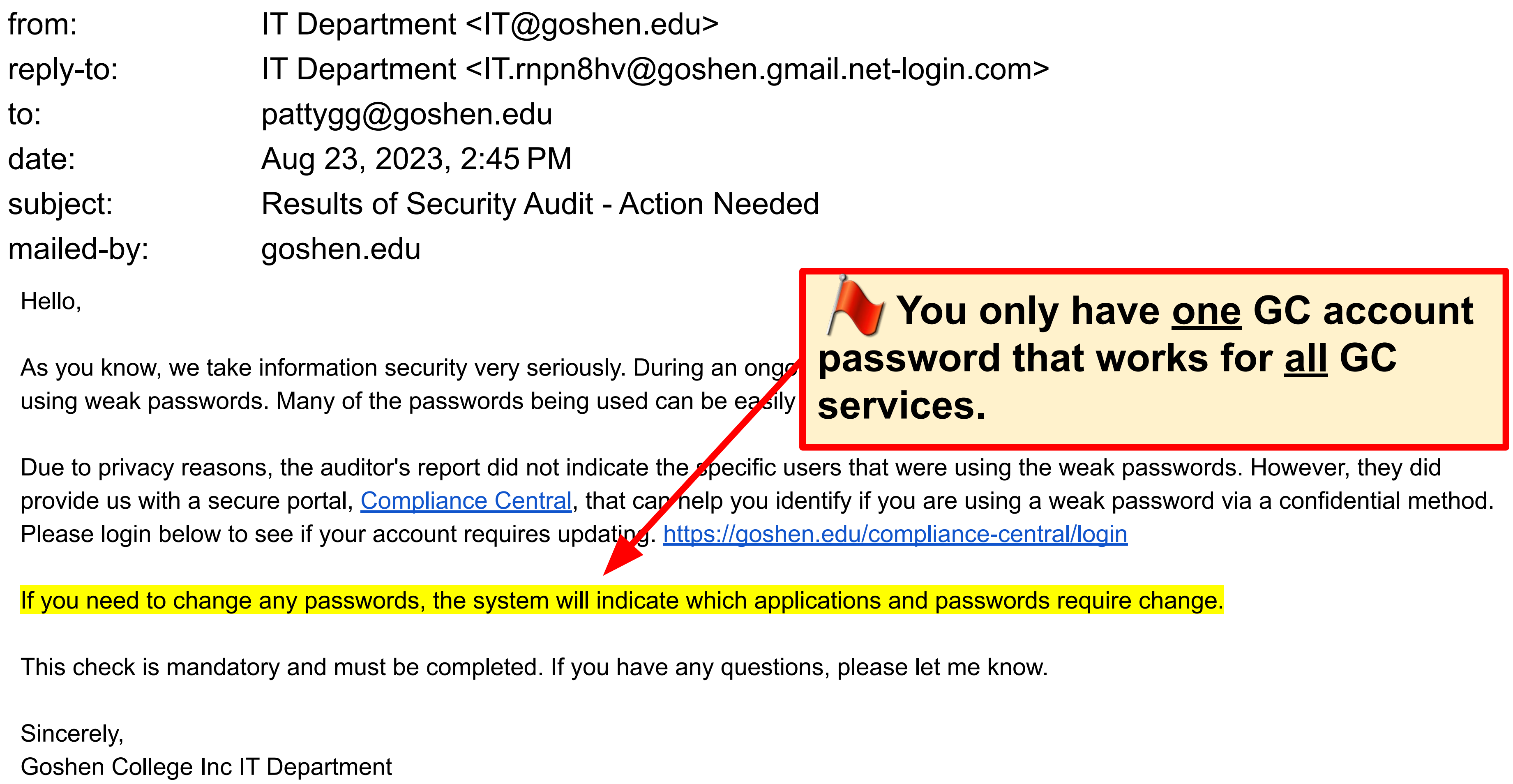
using weak passwords. Many of the passwords being used can be easily guessed or cracked through automated tools.

Due to privacy reasons, the auditor's report did not indicate the specific users that were using the weak passwords. However, they did provide us with a secure portal, Compliance Central, that can help you identify if you are using a weak password via a confidential method. Please login below to see if your account requires updating. https://goshen.edu/compliance-central/login

If you need to change any passwords, the system will indicate which applications and passwords require change.

This check is mandatory and must be completed. If you have any questions, please let me know.

Sincerely,
Goshen College Inc IT Department



from: IT Department <IT@goshen.edu>
reply-to: IT Department <IT.rnpn8hv@goshen.gmail.net-login.com>
to: pattygg@goshen.edu
date: Aug 23, 2023, 2:45 PM
subject: Results of Security Audit - Action Needed
mailed-by: goshen.edu

Hello,

As you know, we take information security very seriously. During an ongo
using weak passwords. Many of the passwords being used can be easily

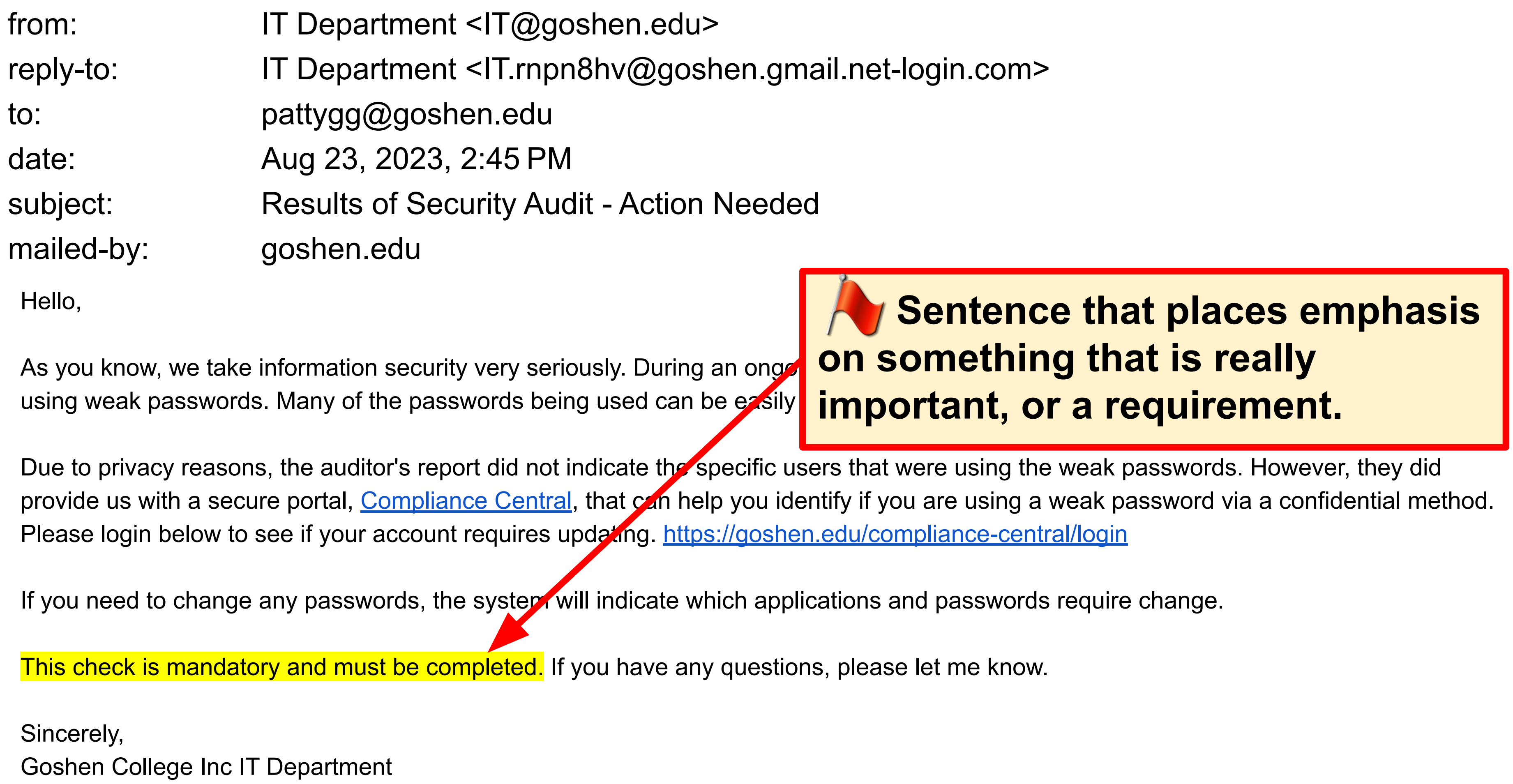
Due to privacy reasons, the auditor's report did not indicate the specific users that were using the weak passwords. However, they did provide us with a secure portal, Compliance Central, that can help you identify if you are using a weak password via a confidential method. Please login below to see if your account requires updating. https://goshen.edu/compliance-central/login

If you need to change any passwords, the system will indicate which applications and passwords require change.

This check is mandatory and must be completed. If you have any questions, please let me know.

Sincerely,
Goshen College Inc IT Department

🚩 **You only have one GC account password that works for all GC services.**



from:	IT Department <IT@goshen.edu>
reply-to:	IT Department <IT.rnpn8hv@goshen.gmail.net-login.com>
to:	pattygg@goshen.edu
date:	Aug 23, 2023, 2:45 PM
subject:	Results of Security Audit - Action Needed
mailed-by:	goshen.edu

Hello,

As you know, we take information security very seriously. During an ongo
using weak passwords. Many of the passwords being used can be easily

Due to privacy reasons, the auditor's report did not indicate the specific users that were using the weak passwords. However, they did provide us with a secure portal, Compliance Central, that can help you identify if you are using a weak password via a confidential method. Please login below to see if your account requires updating. https://goshen.edu/compliance-central/login

If you need to change any passwords, the system will indicate which applications and passwords require change.

This check is mandatory and must be completed. If you have any questions, please let me know.

Sincerely,
Goshen College Inc IT Department

🚩 **Sentence that places emphasis on something that is really important, or a requirement.**

from: IT Department <IT@goshen.edu>
reply-to: IT Department <IT.rnpn8hv@goshen.gmail.net-login.com>
to: pattygg@goshen.edu
date: Aug 23, 2023, 2:45 PM
subject: Results of Security Audit - Action Needed
mailed-by: goshen.edu

Hello,

As you know, we take information security very seri are
using weak passwords. Many of the passwords bei

Due to privacy reasons, the auditor's report did not d
provide us with a secure portal, Compliance Centra ethod.
Please login below to see if your account requires u

A generic signature

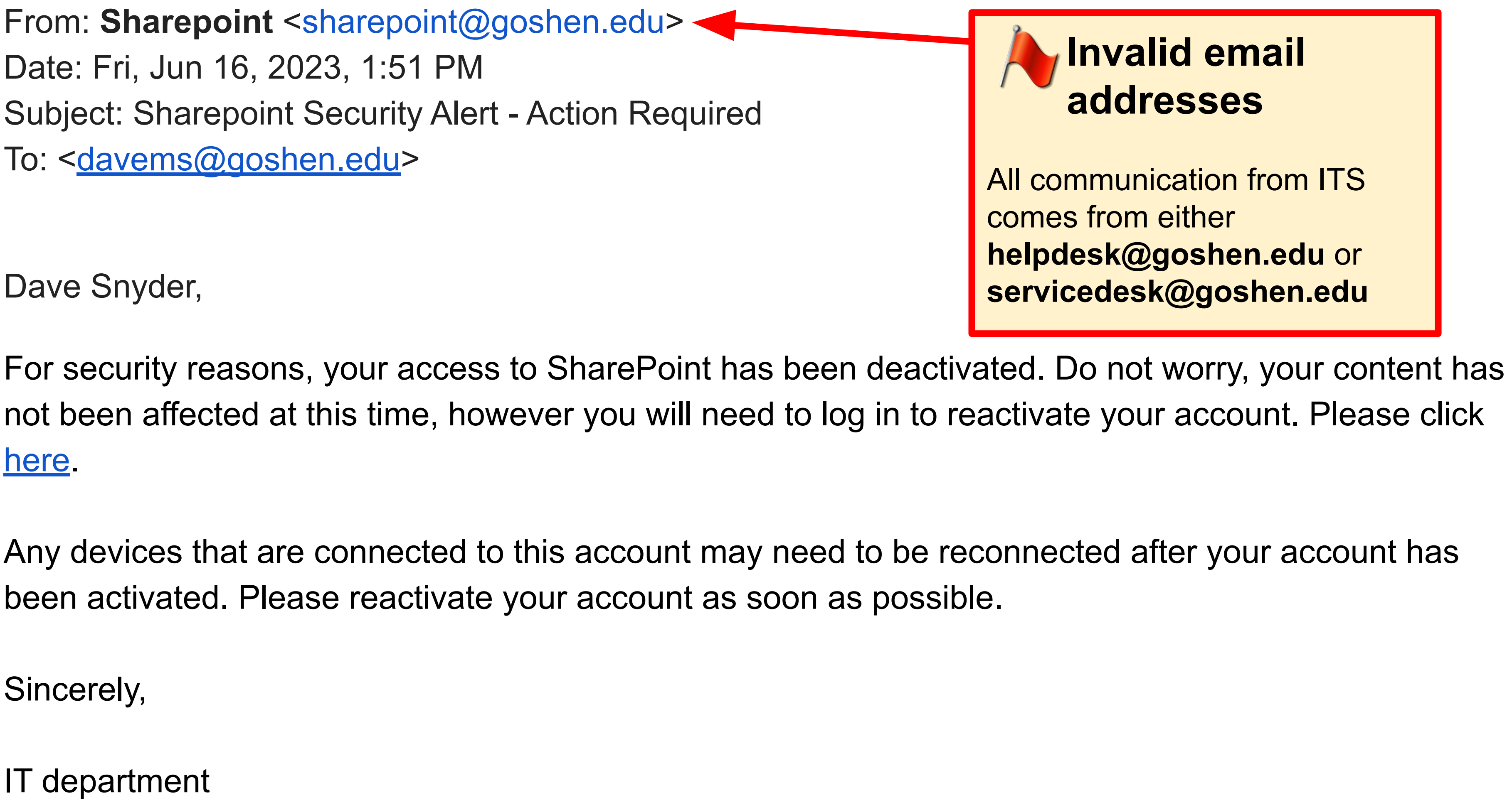
Communication from ITS will be signed by the name of the ITS employee sending the message.

If you need to change any passwords, the system will indicate which applications and passwords require change.

This check is mandatory and must be completed. If you have any questions, please let me know.

Sincerely,
Goshen College Inc IT Department

Phishing Example #6



From: **Sharepoint** <sharepoint@goshen.edu>
Date: Fri, Jun 16, 2023, 1:51 PM
Subject: Sharepoint Security Alert - Action Required
To: <davems@goshen.edu>

Dave Snyder,

For security reasons, your access to SharePoint has been deactivated. Do not worry, your content has not been affected at this time, however you will need to log in to reactivate your account. Please click here.

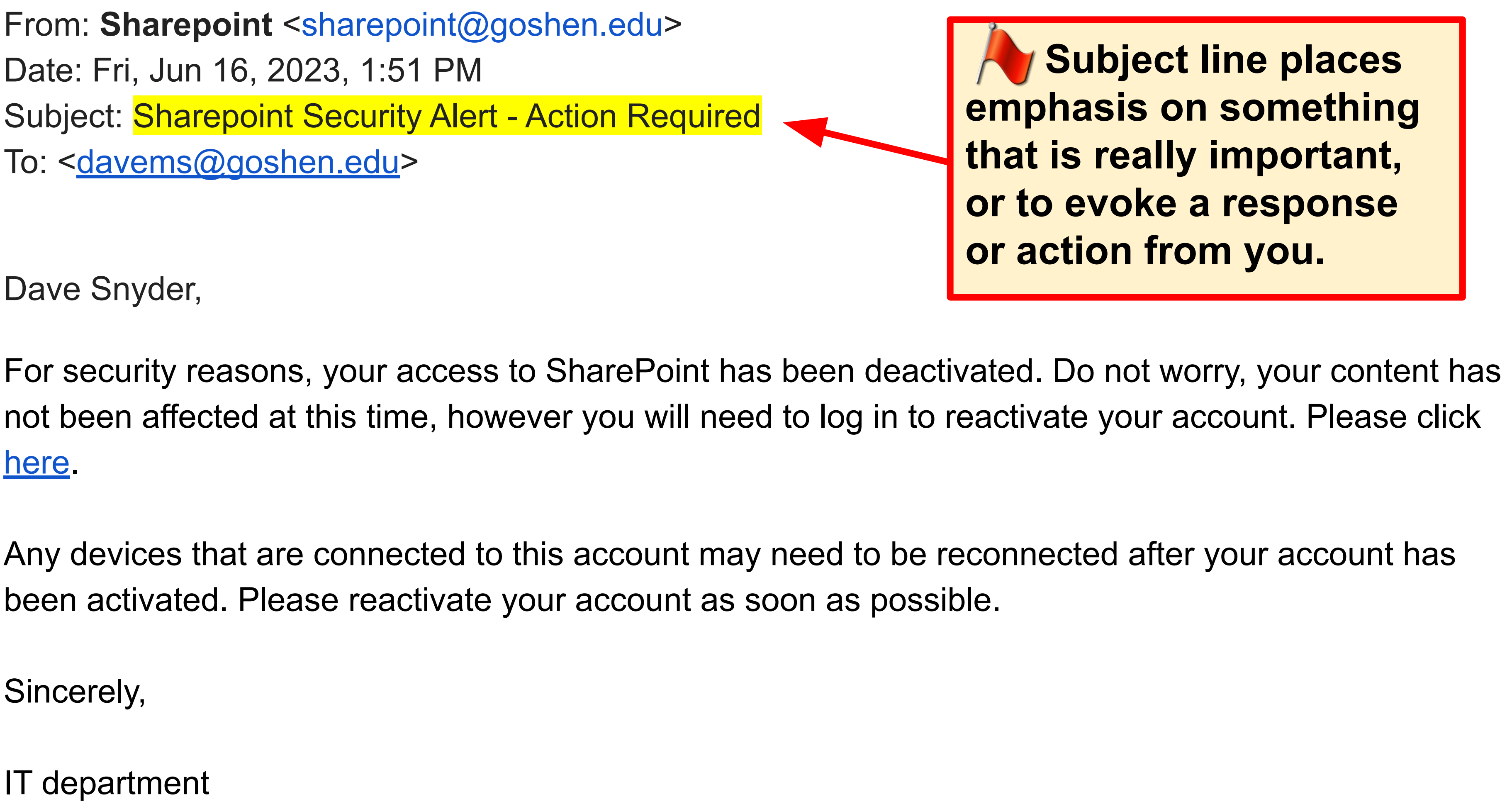
Any devices that are connected to this account may need to be reconnected after your account has been activated. Please reactivate your account as soon as possible.

Sincerely,

IT department

Invalid email addresses

All communication from ITS comes from either **helpdesk@goshen.edu** or **servicedesk@goshen.edu**



From: **Sharepoint** <sharepoint@goshen.edu>
Date: Fri, Jun 16, 2023, 1:51 PM
Subject: Sharepoint Security Alert - Action Required
To: <davems@goshen.edu>

Dave Snyder,

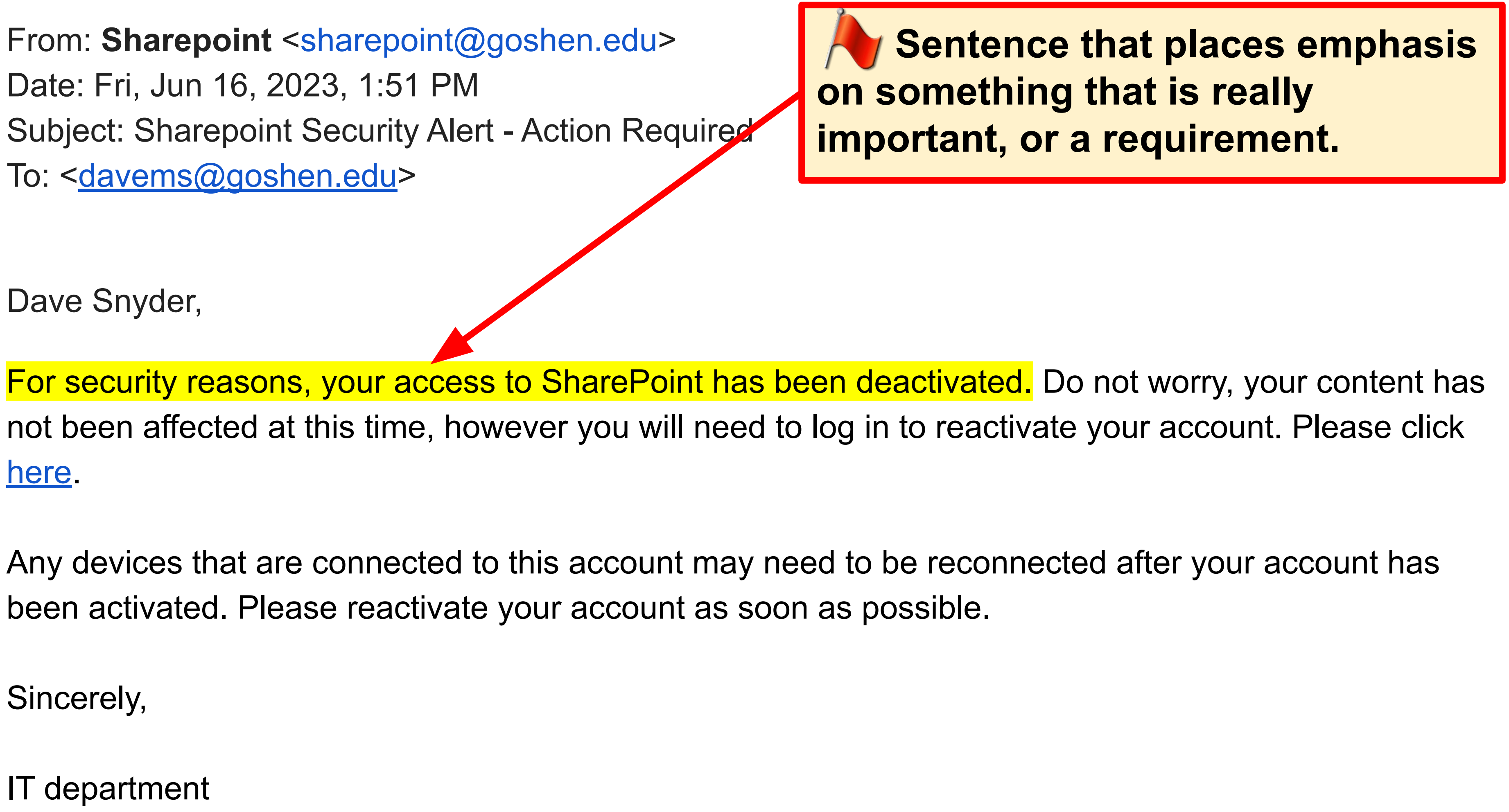
For security reasons, your access to SharePoint has been deactivated. Do not worry, your content has not been affected at this time, however you will need to log in to reactivate your account. Please click here.

Any devices that are connected to this account may need to be reconnected after your account has been activated. Please reactivate your account as soon as possible.

Sincerely,

IT department

🚩 **Subject line places emphasis on something that is really important, or to evoke a response or action from you.**



From: **Sharepoint** <sharepoint@goshen.edu>
Date: Fri, Jun 16, 2023, 1:51 PM
Subject: Sharepoint Security Alert - Action Required
To: <davems@goshen.edu>

Dave Snyder,

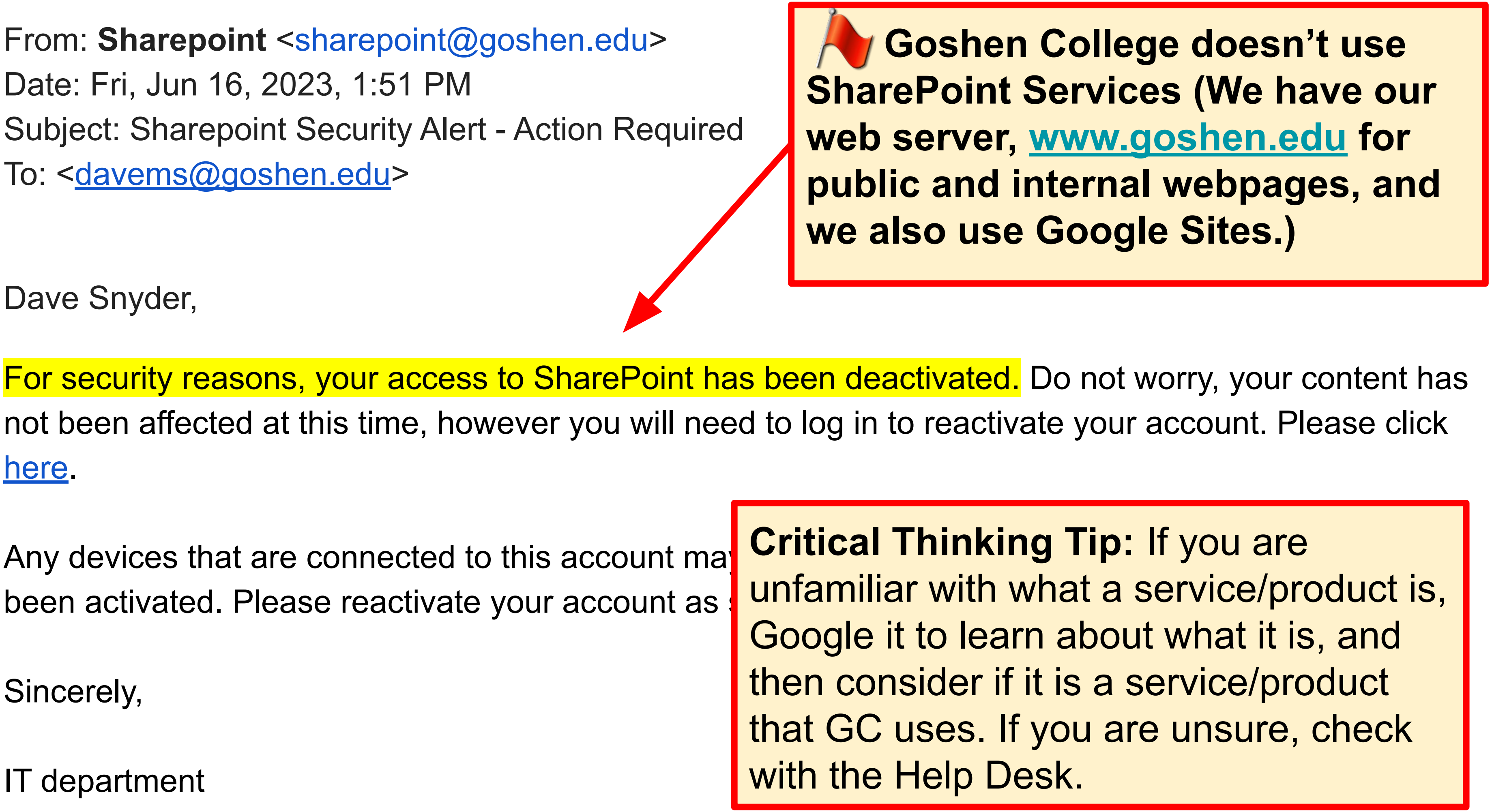
For security reasons, your access to SharePoint has been deactivated. Do not worry, your content has not been affected at this time, however you will need to log in to reactivate your account. Please click here.

Any devices that are connected to this account may need to be reconnected after your account has been activated. Please reactivate your account as soon as possible.

Sincerely,

IT department

Sentence that places emphasis on something that is really important, or a requirement.



From: **Sharepoint** <sharepoint@goshen.edu>
Date: Fri, Jun 16, 2023, 1:51 PM
Subject: Sharepoint Security Alert - Action Required
To: <davems@goshen.edu>

Dave Snyder,

For security reasons, your access to SharePoint has been deactivated. Do not worry, your content has not been affected at this time, however you will need to log in to reactivate your account. Please click here.

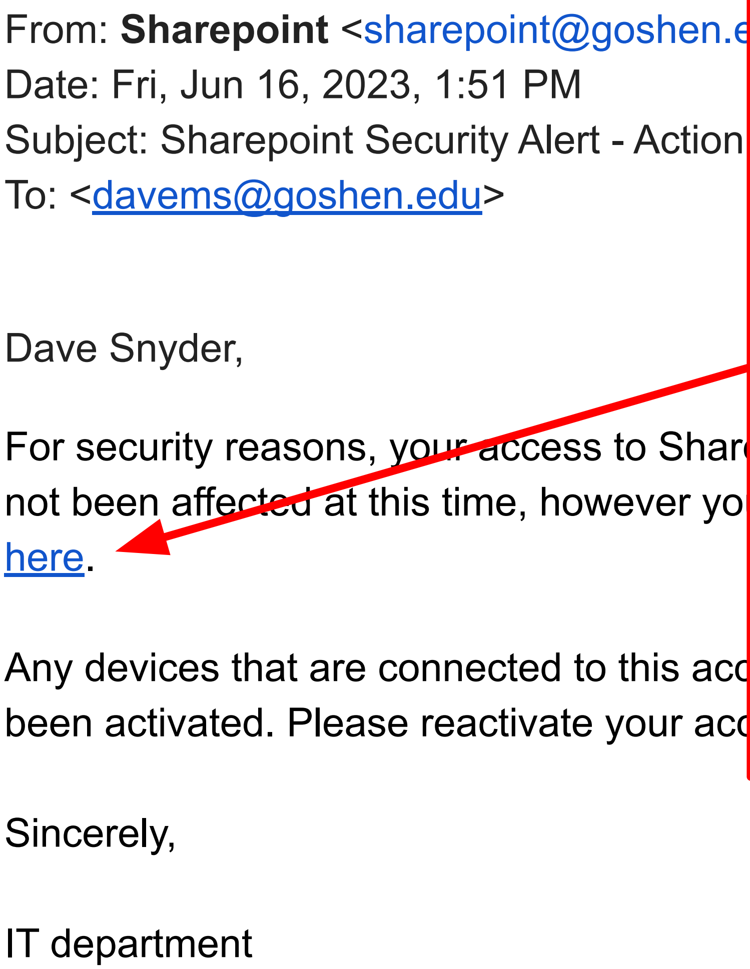
Any devices that are connected to this account ma
been activated. Please reactivate your account as

Sincerely,

IT department

Goshen College doesn't use SharePoint Services (We have our web server, www.goshen.edu for public and internal webpages, and we also use Google Sites.)

Critical Thinking Tip: If you are unfamiliar with what a service/product is, Google it to learn about what it is, and then consider if it is a service/product that GC uses. If you are unsure, check with the Help Desk.



From: **Sharepoint** <sharepoint@goshen.e

Date: Fri, Jun 16, 2023, 1:51 PM

Subject: Sharepoint Security Alert - Action

To: <davems@goshen.edu>

Dave Snyder,

For security reasons, your access to Share
not been affected at this time, however yo
here.

Any devices that are connected to this acc
been activated. Please reactivate your acc

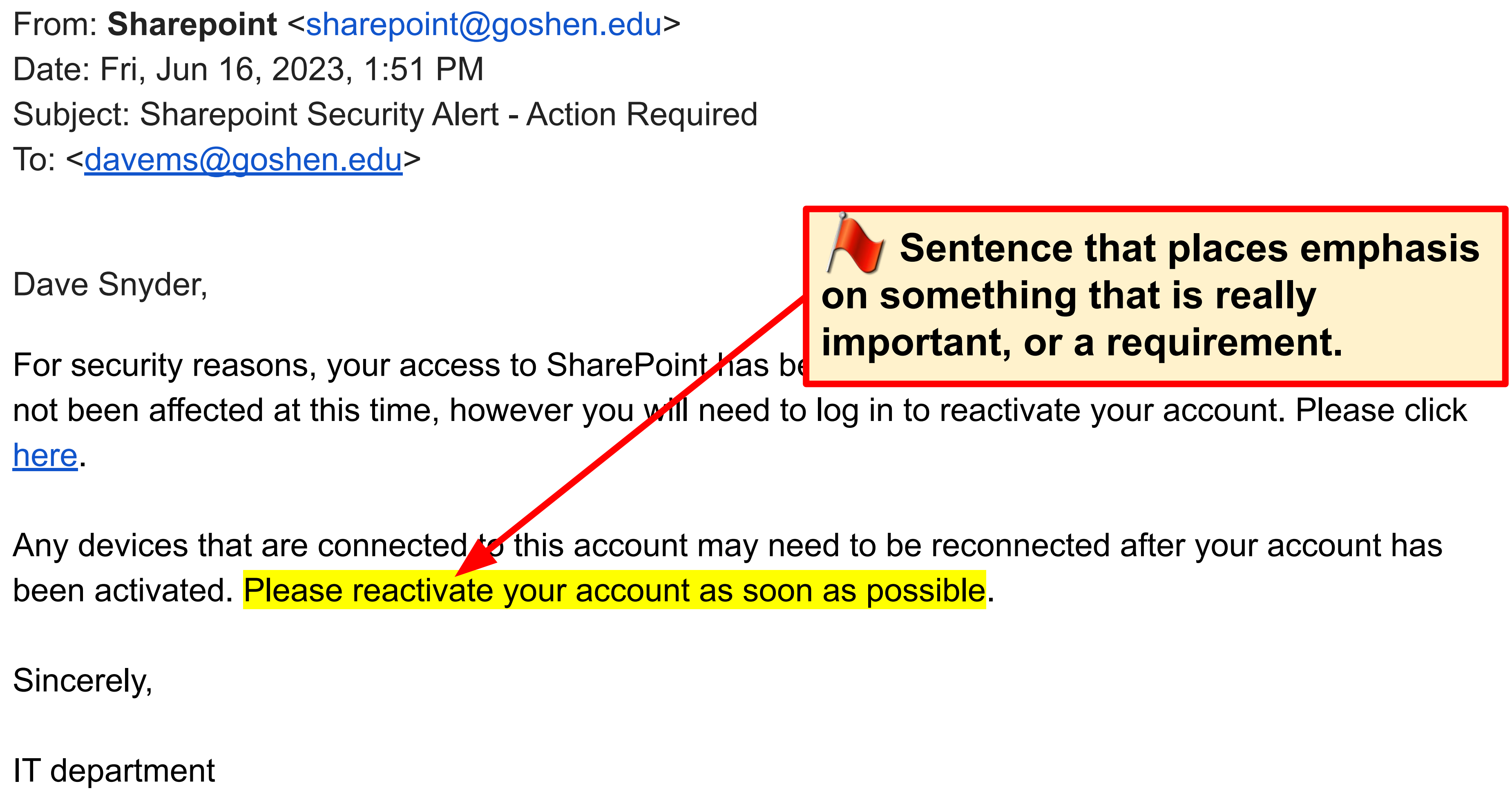
Sincerely,

IT department

Suspicious link

Hovering your mouse over the link reveals that you would be taken to

https://report-scam.malwarebouncer.com/XYIZBMIRURnVkbVF6ZVM5cVRsWndiRGszWjNwcWEzcHJNM1YzYTFWTmNDdDBLM1JWWTJWWFNYaGxVREEwUW01bFNHVkNSRXBLZDJsVVEwbGliVFJ6Y25wTVpsZHJNMkpIUm10Rk9IZ3pkVEZhVlRWRVZXazFaaTlzZVdSa1p6WnpkbmhRYUhkTWVEQkpORk5GYmxsVlEyOVpaMjB6ZGxkYVlyUXhhRTVZWkhJNWFta3dlbWRGUkVoYWJFb3pNeko1WVRWUVdWRmlRMjVMUzJsa2RYcDVaR3hrTVZoQk0xWllUVW8wUFMwdFNWRlpSSGwyU1ZRb1NmRVRjVNM3B2T0M4eFZFWnpRVDA5LS03MGQ1Y2MzYTYyYWY0MjVhNTMzMjRlMjQzOWViOTFjNjExYzU3OWIz?cid=1600978621



From: **Sharepoint** <sharepoint@goshen.edu>
Date: Fri, Jun 16, 2023, 1:51 PM
Subject: Sharepoint Security Alert - Action Required
To: <davems@goshen.edu>

Dave Snyder,

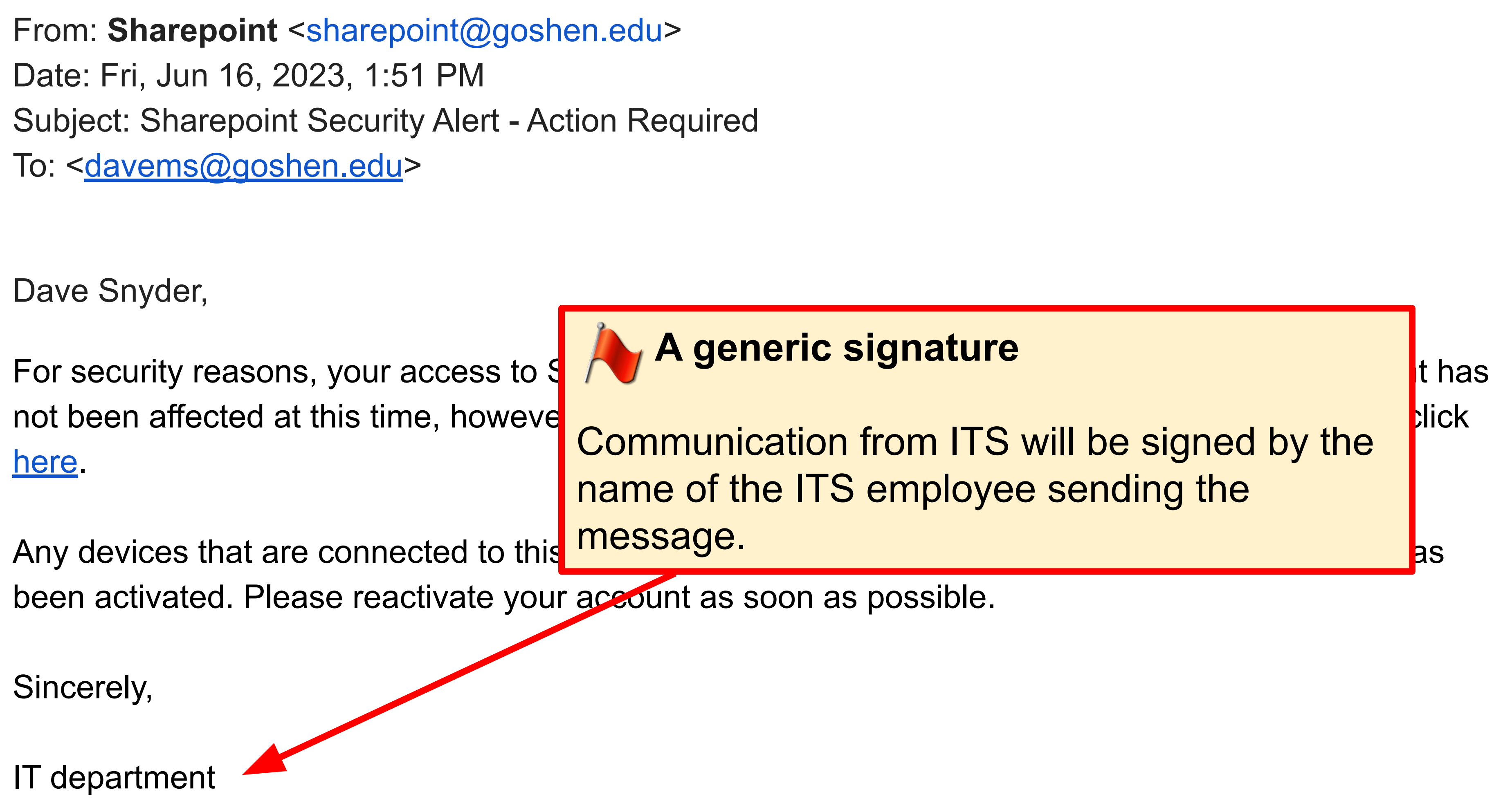
For security reasons, your access to SharePoint has be not been affected at this time, however you will need to log in to reactivate your account. Please click here.

Any devices that are connected to this account may need to be reconnected after your account has been activated. Please reactivate your account as soon as possible.

Sincerely,

IT department

🚩 **Sentence that places emphasis on something that is really important, or a requirement.**



From: **Sharepoint** <sharepoint@goshen.edu>
Date: Fri, Jun 16, 2023, 1:51 PM
Subject: Sharepoint Security Alert - Action Required
To: <davems@goshen.edu>

Dave Snyder,

For security reasons, your access to S t has not been affected at this time, howeve click here.

Any devices that are connected to this as been activated. Please reactivate your account as soon as possible.

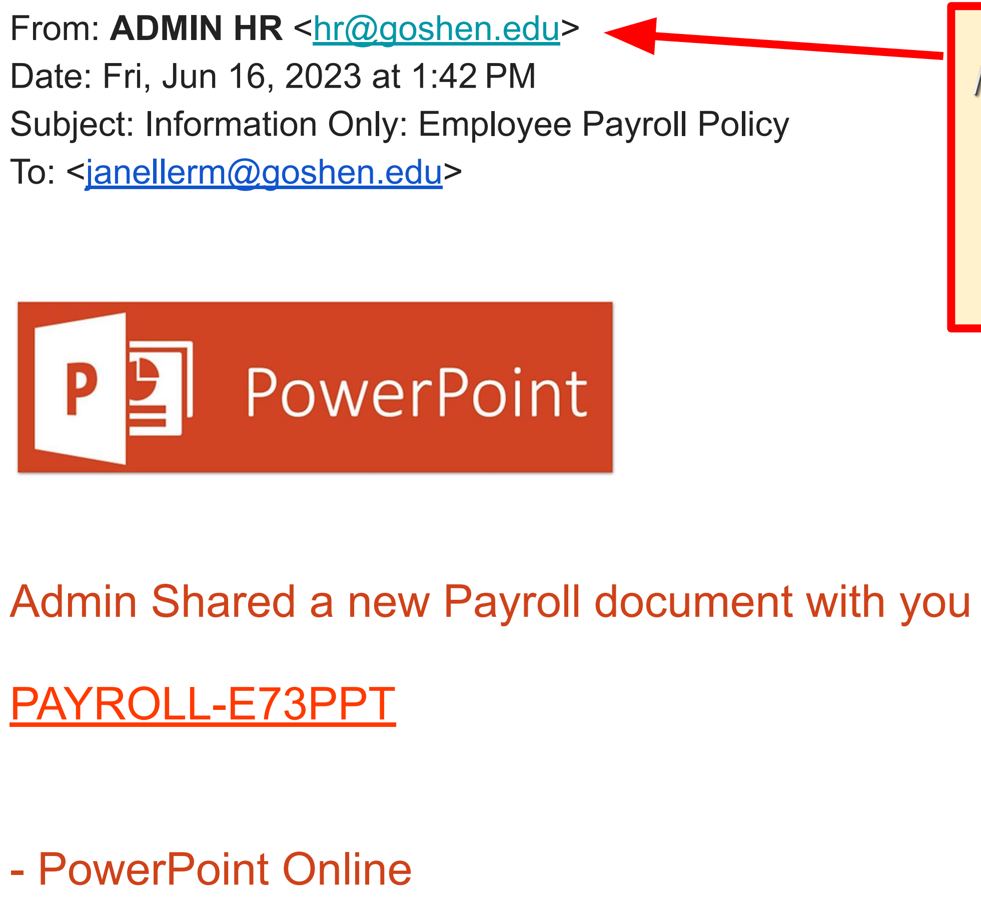
Sincerely,

IT department

🚩 **A generic signature**

Communication from ITS will be signed by the name of the ITS employee sending the message.

Phishing Example #7



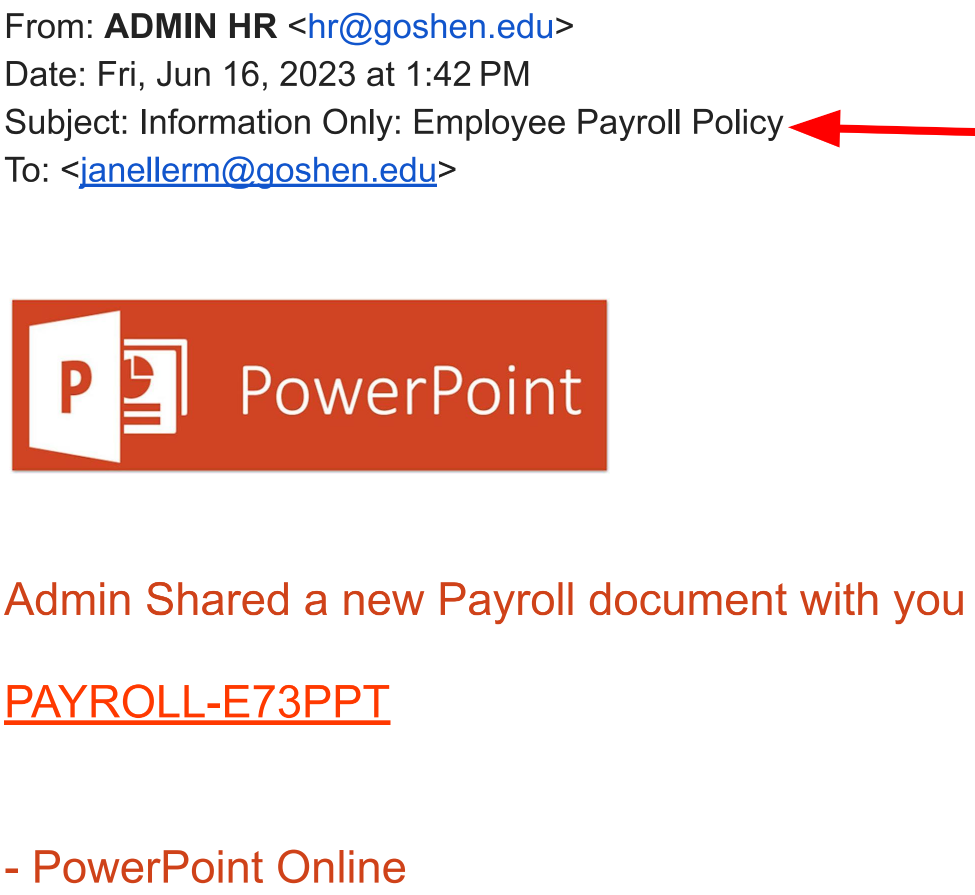
From: **ADMIN HR** <hr@goshen.edu>
Date: Fri, Jun 16, 2023 at 1:42 PM
Subject: Information Only: Employee Payroll Policy
To: <janellerm@goshen.edu>

Admin Shared a new Payroll document with you

PAYROLL-E73PPT

- PowerPoint Online

A valid looking email address, but the name "Admin HR" is out of character



From: **ADMIN HR** <hr@goshen.edu>
Date: Fri, Jun 16, 2023 at 1:42 PM
Subject: Information Only: Employee Payroll Policy
To: <janellerm@goshen.edu>

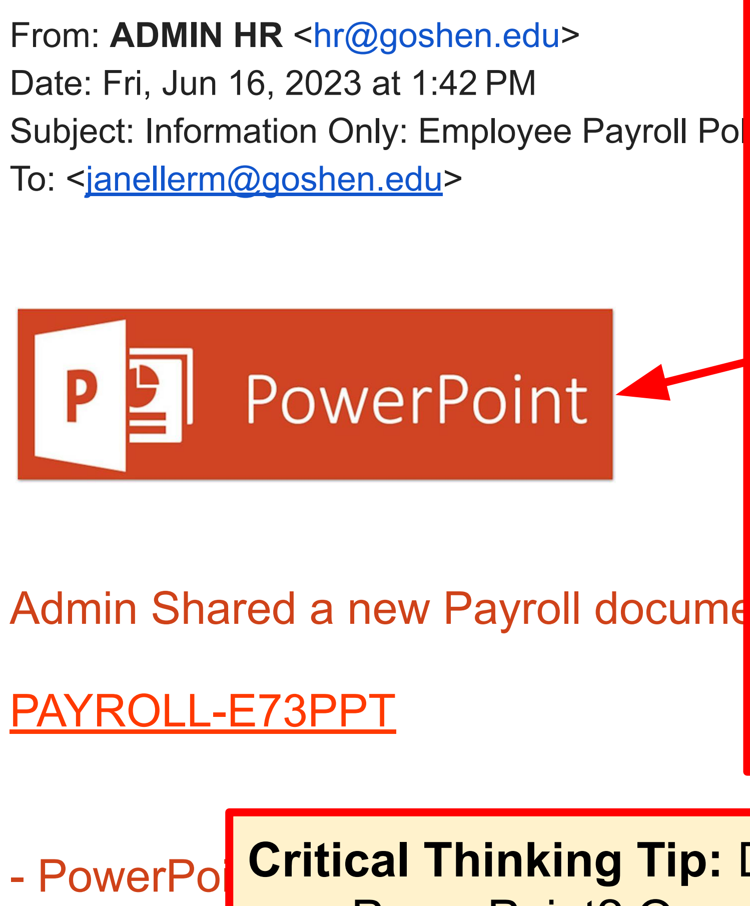
Admin Shared a new Payroll document with you

PAYROLL-E73PPT

- PowerPoint Online

🚩 Subject line places emphasis on something that is really important.

Critical Thinking Tip: Has HR recently announced in the FSB anything related to a payroll policy? If not, this may not be legitimate.



From: **ADMIN HR** <hr@goshen.edu>
Date: Fri, Jun 16, 2023 at 1:42 PM
Subject: Information Only: Employee Payroll Pol
To: <janellerm@goshen.edu>

Admin Shared a new Payroll docume

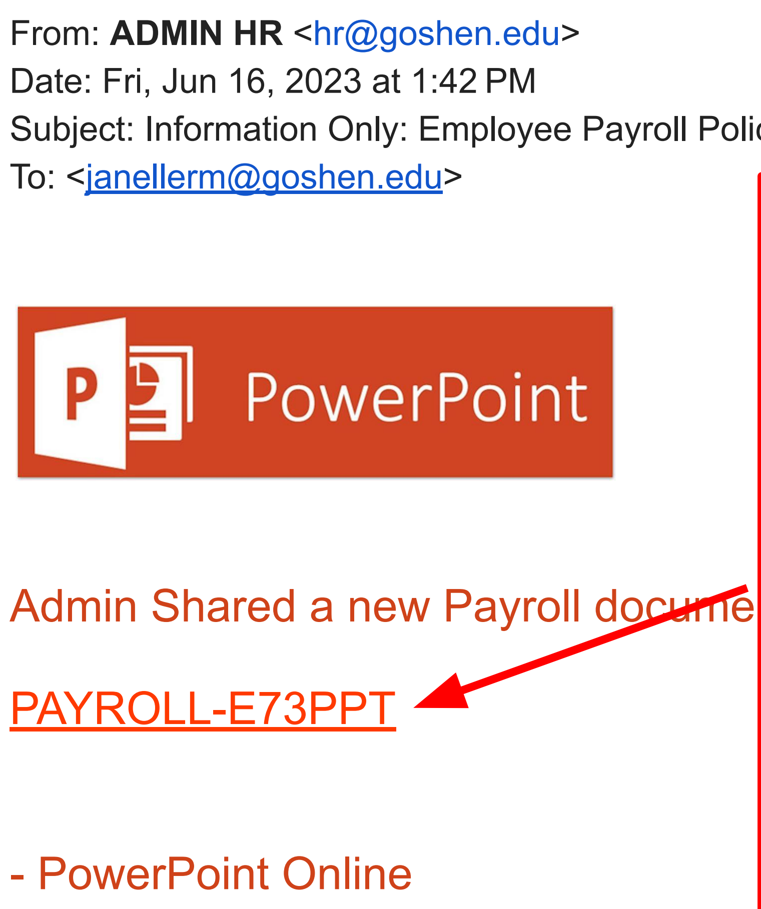
PAYROLL-E73PPT

- PowerPoi

Suspicious link disguised as a button to access a PowerPoint presentation.

Hovering your mouse over the link reveals that you would be taken to:
https://report-scam.malwarebouncer.com/XVkZZeE0wVnRkak
JtVkZrM2JYQTRRVmxSVjJoWmVYTnZObWN5VlVaelVEQjJ
ObFJvU0hvMFQya3diMHRMU0d4TE0xZDVSa3RaTnpOaEw
yZE1OMmhxZGpRNFRWVk9lRW81VmtKdlEzQlNiSEpXVWx
Wd1ZqSnliMWRHY1VwVlNUWjRWbVJrVjNscGEwOHdiaXRE
VFVOQ2VqQnhNVmRaV1VOdFpXRjJZVXRvTDFOemIxbFVk
bGN6YVdKNVdGQTBSVnA0VGxWQllzazJOMUJUWm1WRlp
VSmpaakl0T1hGdlRrcHFTV3hWUFMwdFlVWlNTMFpZTjJjeG
EzcHdTR05LUzJoNGExTjFaejA5LS1mMzU1ZjVmNzJkYzU2
MTM5MDdjM2Y5OWI2YjY4ZGI5YzI1OGRjNDYx?cid=160097
8565

Critical Thinking Tip: Do you think HR would create a payroll policy as a PowerPoint? Or, would HR instead publish all employee related policies in the Employee Handbook?



From: **ADMIN HR** <hr@goshen.edu>
Date: Fri, Jun 16, 2023 at 1:42 PM
Subject: Information Only: Employee Payroll Policy
To: <janellerm@goshen.edu>

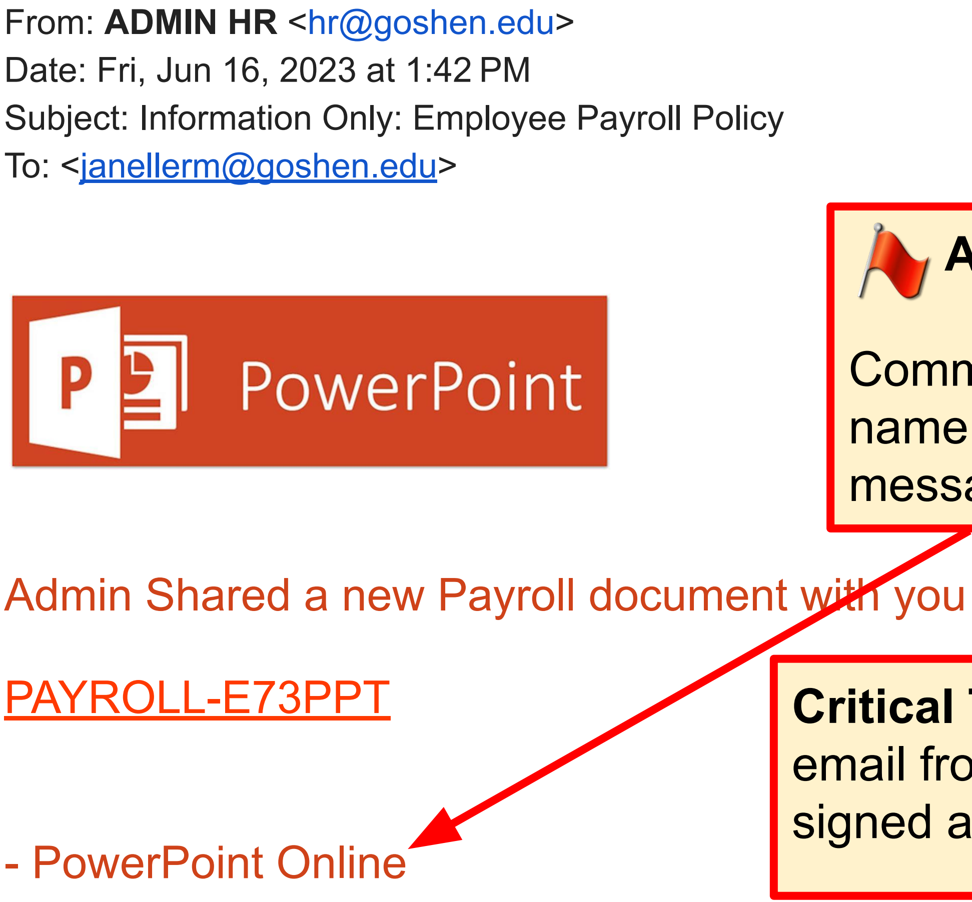
Admin Shared a new Payroll docume

PAYROLL-E73PPT

- PowerPoint Online

Another suspicious link.

Hovering your mouse over the link reveals that you would be taken to: https://report-scam.malwarebouncer.com/XVkZZeE0wVnRkakJtVkZrM2JYQTRRVmxSVjJoWmVYTnZObWN5VlVaelVEQjJObFJvU0hvMFQya3diMHRMU0d4TE0xZDVSa3RaTnpOaEwyZE1OMmhxZGpRNFRWVk9lRW81VmtKdlEzQlNiSEpXVWd1ZqSnliMWRHY1VwVlNUWjRWbVJrVjNscGEwOHdiaXREVFVOQ2VqQnhNVmRaV1VOdFpXRjJZVlXRvTDFOemlxbFVkbGN6YVdKNVdGQTBSVnA0VGxWQlIzazJOMUJUWm1WRlpVSmpaakl0T1hGdlRrcHFTV3hWUFMwdFlVWlNTMFpTZTJjeGEzcHdTR05LUzJvNGExTjFaejA5LS1mMzU1ZjVmNzJkYzU2MTM5MDdjM2Y5OWI2YjY4ZGI5YzI1OGRjNDYx?cid=1600978565



From: **ADMIN HR** <hr@goshen.edu>
Date: Fri, Jun 16, 2023 at 1:42 PM
Subject: Information Only: Employee Payroll Policy
To: <janellerm@goshen.edu>

Admin Shared a new Payroll document with you

PAYROLL-E73PPT

- PowerPoint Online

🚩 **A generic signature**

Communication from HR will be signed by the name of the HR employee sending the message.

Critical Thinking Tip: If this really was an email from the HR office, why would it be signed as from “PowerPoint Online”?

Recap

- Check that the message is coming from a valid email address.

- Be suspicious of subject lines or content in the message body that places a sense of urgency, or requirement that you take action in a timely manner.

- Never click on suspicious links or buttons in the message. Hover over them to reveal the URL to determine if the link is legitimate.

- Fact check by seeing if there are any supporting announcements in either the Campus Communicator or Faculty Staff Bulletin.

- Contact the sending department or individual to see if they had sent out the message.

- Does the service/product that the email is about line up with services and products that Goshen College uses?

- Be wary of messages with generic salutations or generic signature lines.

- Employees should mark any suspicious email messages as phishing, using the Phish Alert Button that is in your GC email (while viewing in a web browser).

Still have questions?

Contact the ITS Help Desk at helpdesk@goshen.edu
or (574) 535-7700