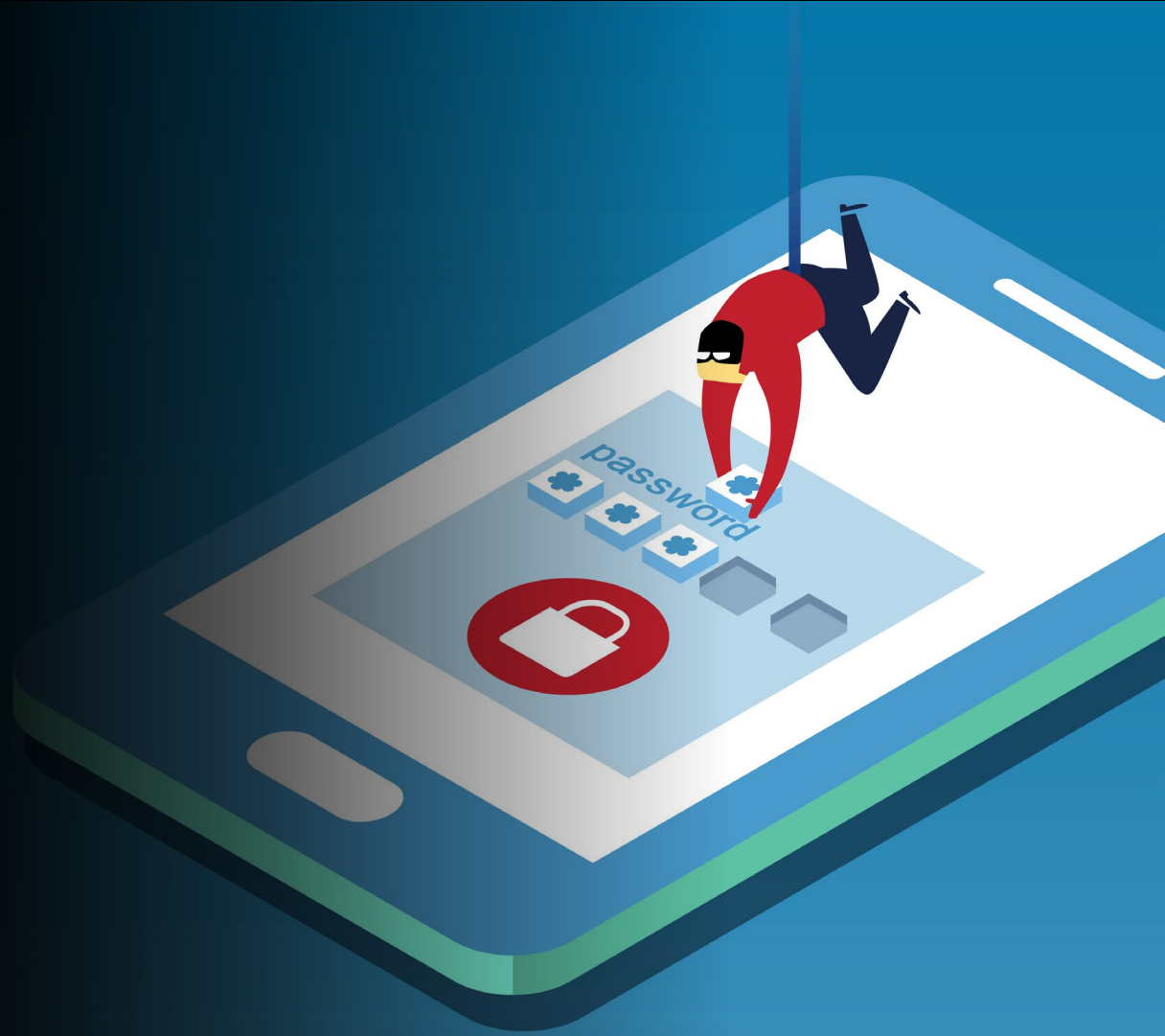


# Phishing and Cybercrime

---



# Phishing

**A kind of internet fraud:**

- email (phishing)
- telephone or voicemail (vishing)
- text message (smishing)

**that seeks to acquire a user's credentials by deception.**

Includes theft of passwords, credit card numbers, bank account details and other confidential information.

Often results in identity theft, financial loss, or reputational and social damage.



# Spear phishing

A specialized form of phishing that targets high value employees or organizations.

Attackers seek to exploit the higher levels of access targets retain.

Goals can include:

- Extortion for money or information
- Tricking or forcing targets into downloading ransomware
- Creating backdoors to organizational infrastructures using malware



# Cybercrime

Cybercrime is **criminal activity that either targets or uses a computer, a computer network or a networked device.**

Most cybercrime is committed by cybercriminals or hackers who want to make money.

Some cybercrime aims to damage computers or networks for reasons other than profit.



# Types of cybercrime

- Email and internet fraud
- Identity fraud
- Financial or CC payment data theft
- Cyberextortion
- Ransomware
- Cyberespionage
- Compromising a network
- Copyright infringement
- Selling illegal items online



# Common fallacious appeals

---

Appeals to authority

---

Appeals to urgency

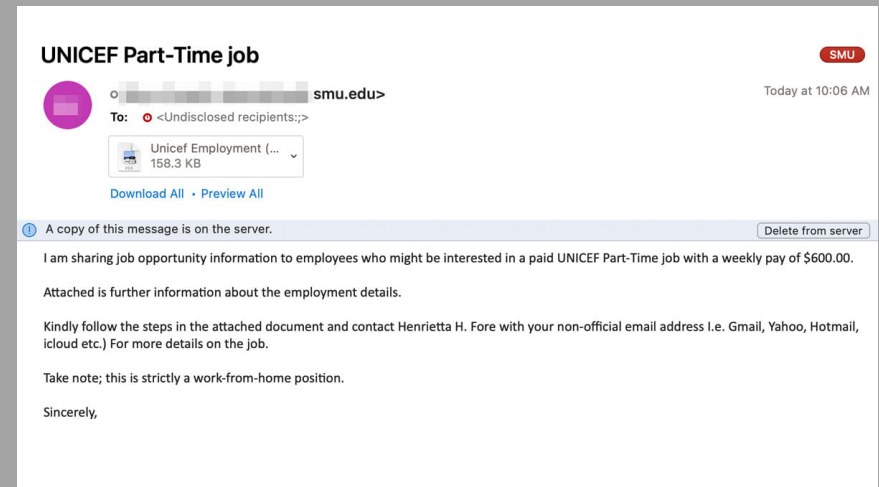
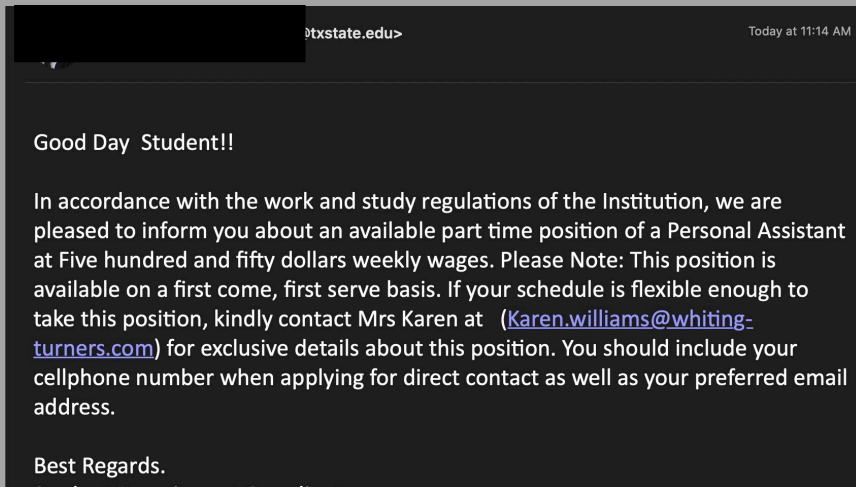
---

Appeals to self-interest

---

Appeals to harm (threats)

# Appeal to self-interest



# Appeals to Authority

---

**From:** CDC-INFO <[REDACTED]@cdc.gov.org>  
**Date:** Tuesday, February 4, 2020 at 10:38 PM  
**To:** [REDACTED]  
**Subject:** 2019-nCoV: Coronavirus outbreak in your city (Emergency)

Distributed via the CDC Health Alert Network  
February 4, 2020  
CDCHAN-00426

Dear [REDACTED],  
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (<https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html>)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,  
CDC-INFO National Contact Center  
National Center for Health Marketing  
Division of eHealth Marketing  
Centers for Disease control and Prevention

**From:** Corona Update <[corona@coronadirect.com](mailto:corona@coronadirect.com)>  
**Subject:** Important Company Corona Virus Update  
**Date:** March 10, 2020 at 12:04:25 PM PDT  
**To:** Privacy <[privacy@\[REDACTED\]](mailto:privacy@[REDACTED])>

Important company update regarding the corona  
Virus has been uploaded to Onedrive.

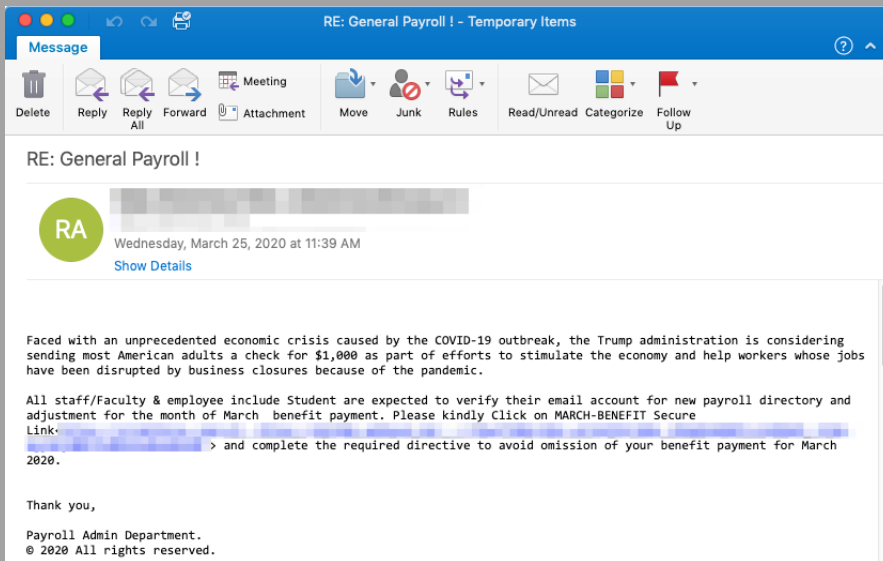
[Login to one drive to action now.](#)

Sincerely,  
Admin




# Appeals to urgency

## Payroll messaging



The screenshot shows an email client window titled "RE: General Payroll ! - Temporary Items". The interface includes a toolbar with icons for Delete, Reply, Reply All, Forward, Attachment, Meeting, Move, Junk, Rules, Read/Unread, Categorize, and Follow Up. The email content is as follows:

RE: General Payroll !

  
RA  
Wednesday, March 25, 2020 at 11:39 AM  
[Show Details](#)

Faced with an unprecedented economic crisis caused by the COVID-19 outbreak, the Trump administration is considering sending most American adults a check for \$1,000 as part of efforts to stimulate the economy and help workers whose jobs have been disrupted by business closures because of the pandemic.

All staff/Faculty & employee include Student are expected to verify their email account for new payroll directory and adjustment for the month of March benefit payment. Please kindly Click on MARCH-BENEFIT Secure Link-  
> and complete the required directive to avoid omission of your benefit payment for March 2020.

Thank you,  
Payroll Admin Department.  
© 2020 All rights reserved.

## Policy messaging

All,

Due to the coronavirus outbreak, [\[\[company\\_name\]\]](#) is actively taking safety precautions by instituting a [Communicable Disease Management Policy](#). This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before [\[\[current\\_date\\_1\]\]](#).

If you have any questions or concerns regarding the policy, please contact [\[\[company\\_name\]\]](#) Human Resources.

Regards,  
Human Resources

# Appeals to harm

I have clips of you watching adult videos



To [redacted]

Reply Reply All

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Hi!

I will be right on point. You visit 18+ sites pretty often and I caught you **satisfying yourself**. Well, we all do it sometimes. How I did this? Your router was vulnerable I v code into the firmware and every device connected on the network including phones were compromised. Then I simply set every device available to record with the c visit 18+ sites. In this moment your router firmware was upgraded by the manufacture so there will be no problems in the future. Also you must to reboot every device to be dumped from the memory on each device because is still active.

Anyway, I got also your contacts lists, phone numbers, emails, social media contacts and here is the deal. If you don't pay me 1300 \$ worth in Bit-Coin, the video with what, will be send to all your contacts.

Amount: **0.14 BTC** (approximately)

My Address Part 1: [redacted]

My Address Part 2: [redacted]

**Important!** My address was split in 2 parts, you must to put the parts together with **no spaces between them** manually using Copy and Paste. The final result after the 1+Part 2) is my final address where you send the coins. You may also save that somewhere to not lose the details.

**Quick tip!** You can buy Bit-Coin from Paxful. Use Google to find it.

From [redacted]

Subject **Use your time wisely 14/12/2018 02:44:26**

11:44 am

To [redacted]

Hi

I run a site in the darkweb, I perform all kinds of services - in the main it is demolition to bussiness and harm. In the main, all but the murder. Often this happens because of unrequited love or competition at bussiness. This month he talked me and set me the order of empty sourness in your face. Standard practice - quickly, hurts, for life. Without too much fuss. I get receive only after finishing the order. So, now I offer you send money to me to be inactive, I suggest this to almost all the victims. If I do n my person will fulfill the mission. If you send me money, in add will provide you the information that I have about the client. A always spend the performer, so I have an option, to get \$1600 fr customer and my inaction, or to receive \$ 4000 from the customer of losing the performer.

I'm getting payments in Bitcoin, its my BTC address - The sum I indicated above. 24 hours to decide and pay.

**Extortion  
Phishing  
Scam**

Message

Delete
 Reply
 Reply All
 Forward
 Attachment
 Meeting
 Switch Background
 Move
 Junk
 Rules
 Read/Unread
 Categorize
 Follow Up

# Your Student Account Refund Has Been Processed



@bgsu.edu>  
 To: <Undisclosed recipients:;>

Friday, August 14, 2020 at 11:22 AM

Hello,  
 Your refund has been processed:  
**Refund Details**

Payment Method: Primary Checking  
 Refund Amount: \$1,655.50

Please allow up to 5 business days for the funds to be deposited into your bank account. If the refund amount is not reflected within the 5 business days, log in to your Bursar Account Suite through [CatsWeb](#) and verify the routing and account numbers you have entered for that account. If correct, please contact your financial institution and verify with them that your account and routing information is accurate.

To be safe, please check now through [CatsWeb](#)

Please do not respond to this email. If you have a question, please go to <http://studentinfo.txstate.edu> and either search the FAQs or select "Ask A Question" and you will be assisted.

*TXState Bursar's Office*

**From:** Corona Update <[corona@coronadirect.com](mailto:corona@coronadirect.com)>  
**Subject:** Important Company Corona Virus Update  
**Date:** March 10, 2020 at 12:04:25 PM PDT  
**To:** Privacy <[privacy@\[redacted\]](mailto:privacy@[redacted])>

Important company update regarding the corona Virus has been uploaded to Onedrive.

[Login to one drive to action now.](#)

Sincerely,  
Admin

## Memo From The HR Department



[\[redacted\]](#) @txstate.edu>

To: ● noreply@txstate.edu

Hello,

You have a message from the HR Department

[Click here to view your message](#)

## From The HR Department

  
BT

Greetings,

You have a message from the HR Department


Click [HERE](#) to view your message

Office 865-594-1800 | Fax 865-594-1822

Copyright©2022 CCU All rights reserved.

# Red Flags

**Campus funding/U.S Govt Educational Grant (Submit Application)** ☰

To:  <@txstate.edu> ← Poor writing convention

Friday, October 2, 2020 at 4:49 PM

**Campus Benefit funding.** ← Poor writing convention

Have you experienced a hardship related to the disruption on-campus operations due to COVID-19 that resulted in reduced income or extra expenses? Maybe we can help you. Emotional appeal

Student eligibility for Federal Emergency Relief Grants

The Federal Coronavirus Aid, Relief and Economic Security (CARES) Act has made funding available to colleges and universities to assist eligible students who have been impacted by an on-campus COVID-19 financial disruption. The estimated total number of students at the institution eligible to participate in programs under Section 484 in Title IV of the Higher Education Act of 1965 and therefore eligible to receive an emergency financial aid grant is 100,714.

Students who received a Federal Pell grant at during the spring 2020 semester will automatically be considered for funding with these additional conditions (no application is required):

- Must be a U.S. citizen or eligible non-citizen.
- Must be registered with Selective Service, if required.
- Must not be in default, owe a refund or repayment to a federal financial aid program.
- Must be enrolled in a degree seeking program.
- Have not been convicted for the sale of or possession of an illegal drug offense that occurred while you were receiving federal student aid.
- Must be enrolled in classes for the summer 2020 and/or fall 2020 semesters.
- Funding from the CARES Act is limited. Not all students may receive an award.

Students who are not Federal Pell grant eligible can be considered for funding if they meet the following criteria:

Submit an application for emergency funding.

- Must be a U.S. citizen or eligible non-citizen.
- Males must be registered with Selective Service, if required.
- Must not be in default, owe a refund or repayment to a federal financial aid program.
- Must be enrolled in a degree seeking program.
- Have not been convicted for the sale or possession of an illegal drug offense that occurred while you were receiving federal student aid.

Deceptive blend of real and fraudulent information designed to frame the social engineering aspect of this phishing inside of a seemingly legitimate communication in order to bypass a victim's sense of scrutiny.

**Consumer information**

The Federal CARES Act, Section 18004, Higher Education Emergency Relief Fund, allows schools to consider students for federal emergency financial aid grants for: expenses related to the disruption of campus operations due to corona virus including eligible expenses under a student's cost of attendance, such as food, housing, course materials, technology (including the purchase or replacement of a personal computer), health care and child care.

Federal funding for the Emergency Relief Grant is limited and will be awarded to eligible students meeting the consideration criteria.  
The Federal Emergency Relief Grant program may likely not meet your full financial need.  
This is a one-time grant and is not renewable.

Two sections both titled "Consumer information" The section first gives seemingly accurate information and cites the CARES act. The second section again gives an emotional appeal just before the "application ink" is provided below.

**Consumer information**

The Emergency Relief Funds allow the university to consider students for emergency financial aid grants for: expenses related to the disruption of campus operations due to coronavirus including eligible expenses under a student's cost of attendance, such as food, housing, course materials, technology (including the purchase or replacement of a personal computer), health care and child care.

Campus funding is limited and will be awarded to eligible students meeting the consideration criteria.  
The funding may likely not meet your full financial expectations.  
This is one-time funding and is not renewable.

**Grant value and receipt of funds**

The value of this grant may vary up to \$15,000 based upon your unique circumstances. A grant offered will be paid to you through direct deposit or a mailed check.

Individuals can apply to gain access to the Campus Benefit funding by [CLICKING HERE](#) ← Emotional appeal and sense of urgency followed by a call to action.

Thanks.

# Identifying phishing

- Know who is contacting you
- Don't be reactive
- Inspect hyperlinks
- Avoid attachments

Your Student Account Refund Has Been Processed - Temporary Items

Forward Meeting Attachment Switch Background Move Junk Rules Read/Unread Categorize Follow Up

### Student Account Refund Has Been Processed

Friday, August 14

To: <Undisclosed recipients:>

refund has been processed:  
fund Details

Payment Method: Primary Checking  
Refund Amount: \$1,655.50

Please allow up to 5 business days for the funds to be deposited into your bank account. If the refund amount is not received within the 5 business days, log in to your Bursar Account Suite through [CatsWeb](#) and verify the routing and account numbers for that account. If correct, please contact your financial institution and verify with them that your account and routing information is accurate.

To be safe, please check now through [CatsWeb](#). Please do not respond to this email. If you have a question, please go to <http://studentinfo.txstate.edu> and either search for your question or select "Ask A Question" and you will be assisted.

*TXState Bursar's Office*

make seem shy

Always be cautious of the words "verify your account," or phrases like it. Remember to hover over hyperlinks

Remember to hover over hyperlinks

This is not an email from an official channel, it's also not even from Texas State University

This is a red flag - no actual email signature and the use of the word "Bursar's Office." While "bursar" has a valid meaning, this is not the name of the office.

Message

Delete Reply Reply All Forward Attachment Meeting Switch Background Move Junk Rules Read/Unread Categorize Follow Up

## Your Student Account Refund Has Been Processed



RS @bhdsu.edu  
 To: <Undisclosed recipients;>

Friday, August 14, 2020 at 11:22 AM

It is unusual to include exact amounts in an email

Hello,  
 Your refund has been processed:  
**Refund Details**

This is not an email from an official channel, it's also not even from Texas State University

Payment Method: Primary Checking  
 Refund Amount: \$1,655.50

Always be cautious of the words "verify your account," or phrases like it. Remember to hover over hyperlinks

This is a red flag - an emotional appeal to "be safe" might make this email seem trustworthy

Please allow up to 5 business days for the funds to be deposited into your bank account. If the refund amount is not reflected within the 5 business days, log in to your Bursar Account Suite through [CatsWeb](#) and verify the routing and account numbers you have entered for that account. If correct, please contact your financial institution and verify with them that your account and routing information is accurate.

To be safe, please check now through [CatsWeb](#)

Please do not respond to this email. If you have a question, please go to <http://studentinfo.txstate.edu> and either search the FAQs or select "Ask A Question" and you will be assisted.

**TXState Bursar's Office**

Remember to hover over hyperlinks

This is a red flag - no actual email signature and the use of the word "Bursar's Office." While "bursar" has a valid meaning, this is not the name of the office.

Remember to hover over hyperlinks



# Campus funding/U.S Govt Educational Grant (Submit Application)



Redacted personal email @txstate.edu>  
To: [Redacted]

Poor writing convention

Friday, October 2, 2020 at 4:49 PM

Campus Benefit funding,

Poor writing convention

Have you experienced a hardship related to the disruption on-campus operations due to COVID-19 that resulted in reduced income or extra expenses? Maybe we can help you.

Emotional appeal

Student eligibility for Federal Emergency Relief Grants

The Federal Coronavirus Aid, Relief and Economic Security (CARES) Act has made funding available to colleges and universities to assist eligible students who have been impacted by an on-campus COVID-19 financial disruption. The estimated total number of students at the institution eligible to participate in programs under Section 484 in Title IV of the Higher Education Act of 1965 and therefore eligible to receive an emergency financial aid grant is 100,714.

Students who received a Federal Pell grant at during the spring 2020 semester will automatically be considered for funding with these additional conditions (no application is required):

- Must be a U.S. citizen or eligible non-citizen.
- Must be registered with Selective Service, if required.
- Must not be in default, owe a refund or repayment to a federal financial aid program.
- Must be enrolled in a degree seeking program.
- Have not been convicted for the sale of or possession of an illegal drug offense that occurred while you were receiving federal student aid.
- Must be enrolled in classes for the summer 2020 and/or fall 2020 semesters.
- Funding from the CARES Act is limited. Not all students may receive an award.

Deceptive blend of real and fraudulent information designed to frame the social engineering aspect of this phishing inside of a seemingly legitimate communication in order to bypass a victim's sense of scrutiny.

Students who are not Federal Pell grant eligible can be considered for funding if they meet the following criteria:

Submit an application for emergency funding.

- Must be a U.S. citizen or eligible non-citizen.
- Males must be registered with Selective Service, if required.
- Must not be in default, owe a refund or repayment to a federal financial aid program.
- Must be enrolled in a degree seeking program.
- Have not been convicted for the sale or possession of an illegal drug offense that occurred while you were receiving federal student aid.



### Consumer information

The Federal CARES Act, Section 18004, Higher Education Emergency Relief Fund, allows schools to consider students for federal emergency financial aid grants for: expenses related to the disruption of campus operations due to corona virus including eligible expenses under a student's cost of attendance, such as food, housing course materials, technology (including the purchase or replacement of a personal computer), health care and child care.

Federal funding for the Emergency Relief Grant is limited and will be awarded to eligible students meeting the consideration criteria.  
The Federal Emergency Relief Grant program may likely not meet your full financial need.  
This is a one-time grant and is not renewable.

Two sections both titled "Consumer information"  
The section first gives seemingly accurate information and cites the CARES act. The second section again gives an emotional appeal just before the "application link" is provided below.

### Consumer information

The Emergency Relief Funds allow the university to consider students for emergency financial aid grants for: expenses related to the disruption of campus operations due to coronavirus including eligible expenses under a student's cost of attendance, such as food, housing, course materials, technology (including the purchase or replacement of a personal computer), health care and child care.

Campus funding is limited and will be awarded to eligible students meeting the consideration criteria.  
The funding may likely not meet your full financial expectations.  
This is one-time funding and is not renewable.

### Grant value and receipt of funds

The value of this grant may vary up to \$15,000 based upon your unique circumstances. A grant offered will be paid to you through direct deposit or a mailed check.

individuals can apply to gain access to the Campus Benefit funding by [CLICKING HERE](#)

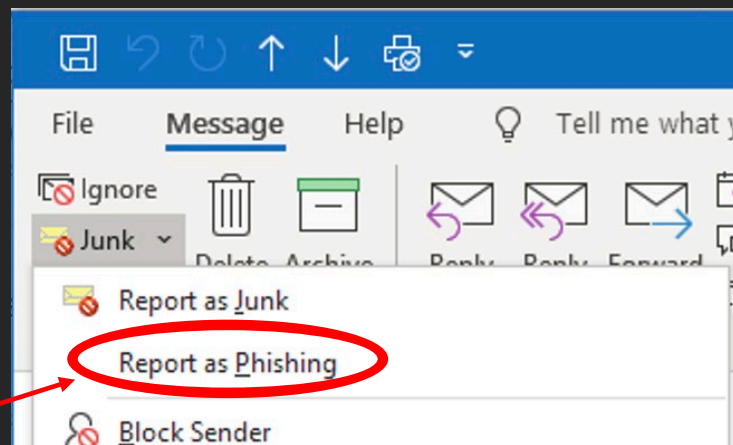


Emotional appeal and sense of urgency followed by a call to action.

Thanks.

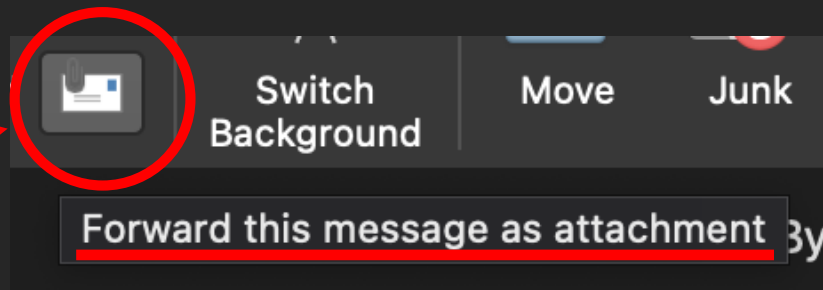
# Reporting Phishing Emails

Suspected or known phishing emails should either be reported as phishing using the feature in the Microsoft email client or be forwarded as an attachment to [abuse@txstate.edu](mailto:abuse@txstate.edu).



Two options for reporting

1. Report as phishing
2. Forward as an attachment



# Fraudulent Login pages

Please see the attached invoice

Sign in with your office 365 e-mail account to view attached pdf.

 Microsoft

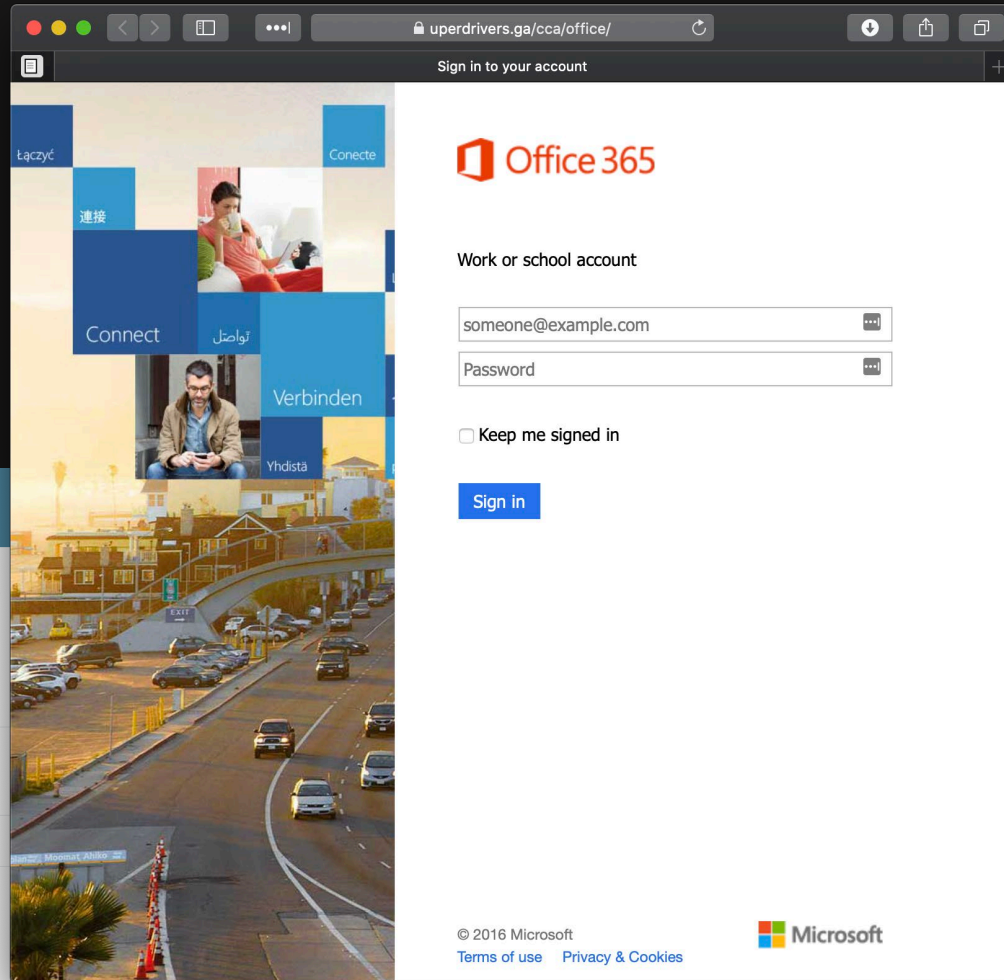
1. Email address \*

2. Password \*

This document is protected. Please enter your valid credentials to review.

Submit

0%



The screenshot shows a browser window with the URL `uperdrivers.ga/cca/office/`. The page is titled "Sign in to your account" and features the Office 365 logo. The background is a collage of images with various "Connect" labels in different languages: "Łączyć", "Connecte", "连接", "Connect", "تواصل", "Verbinden", and "Yhdista". The login form includes a "Work or school account" section with an email input field containing "someone@example.com" and a password input field. There is a "Keep me signed in" checkbox and a "Sign in" button. At the bottom, it displays "© 2016 Microsoft" and links for "Terms of use" and "Privacy & Cookies".

 Office 365

Work or school account

someone@example.com

Password

Keep me signed in

Sign in

© 2016 Microsoft  
[Terms of use](#) [Privacy & Cookies](#)

 Microsoft

TEXAS STATE UNIVERSITY

To all Students and Staffs at Texas State University, kindly validate your account to view new files.

User ID

Password

**Submit** Never give out your password. Don't give your personal information to someone you don't trust.

Powered by Microsoft Excel

[Terms of Use](#) | [Privacy and Cookies](#) | [Help Improve Office](#)

Microsoft

← [redacted]@txstate.edu

**Enter password**

Because you're accessing sensitive info, you need to verify your password...

Password  Draft

[Forgot my password](#)

**Sign in**

UNIVERSAL®

**EMPLOYMENT OPPORTUNITY!!!**

screenshot-result

**Application Form**

Please ensure that you fill in your correct information. We will reply within 24 hours!

Full Name\*

House Address\*

City\*

State\*

Zip Code\*

Personal Email\*

Phone #\*

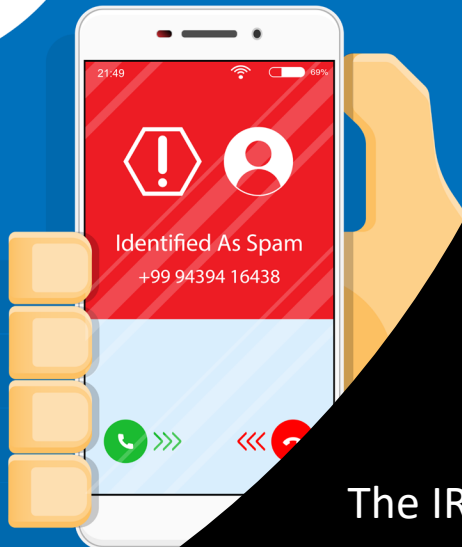
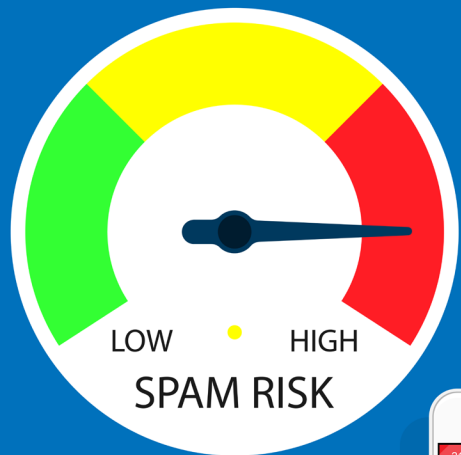
Employment Status\*

Age\*

I'm not a robot

**APPLY NOW**

Copyright © All Rights Reserved



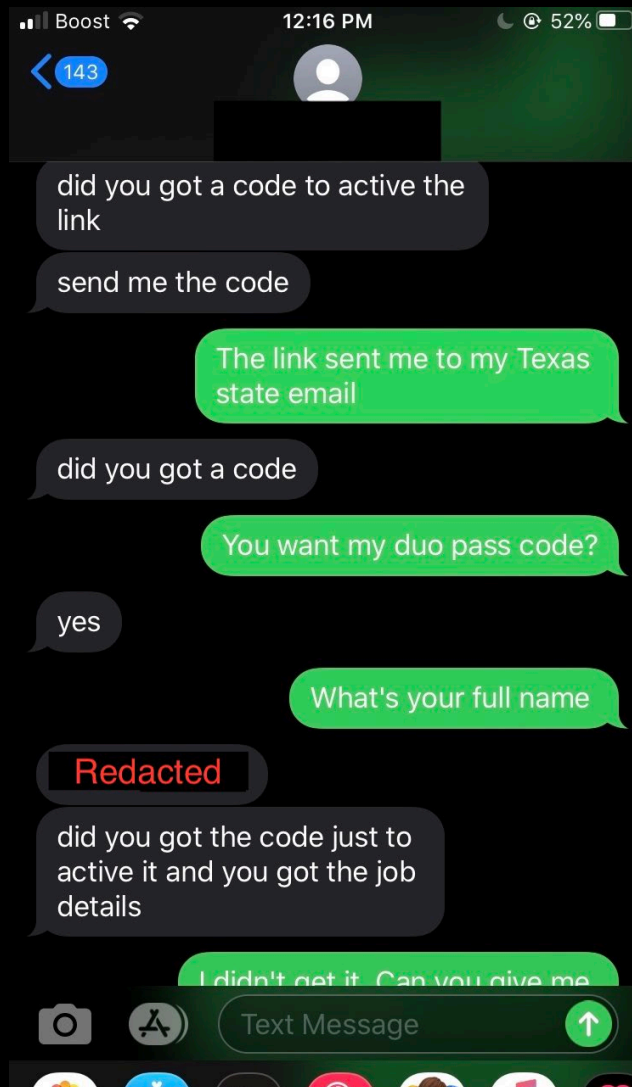
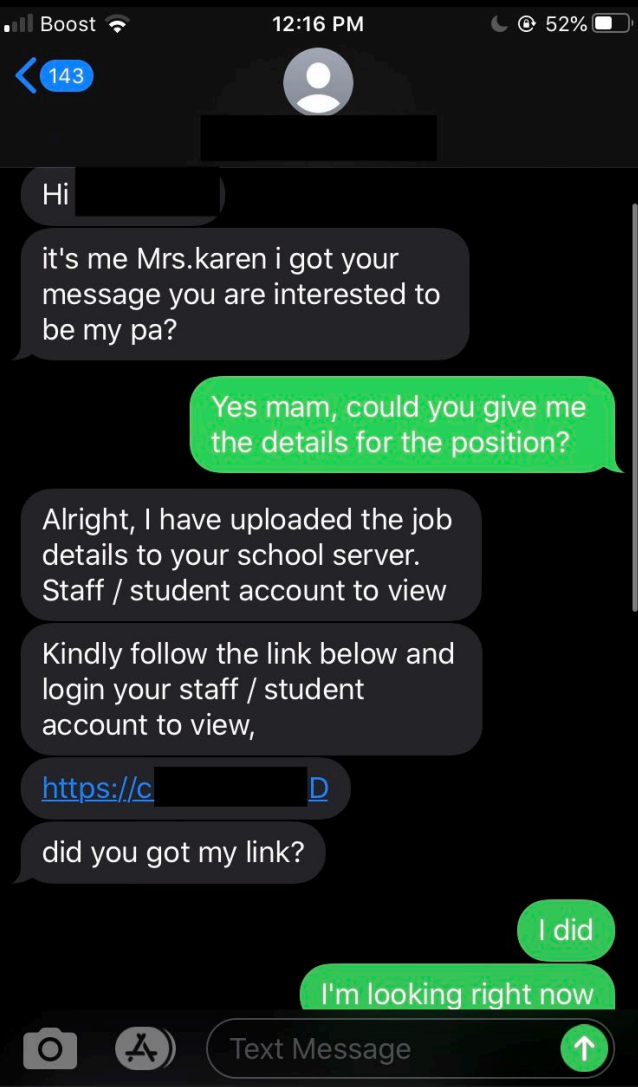
# Phishing and Vishing

Do not respond to unknown numbers.

Never share your personal or financial information.

Be resolute when being pressured to share any information or make a payment.

The IRS, FBI, TXST, etc., **will never call you** to ask for personal info or money.



Smishing / Social Engineering



# Best Practices



# Good Password Hygiene



# Password Manager and MFA

# Resources

Gartner Group: [www.gartner.com](http://www.gartner.com)

- Business reviews, magic quadrant

Dark Reading: <http://www.darkreading.com/>

- Database and application security, technical security threats

OWASP: <https://owasp.org>

- Secure software development resources

SANS: [www.sans.org](http://www.sans.org)

- security training and GIAC certification

(ISC)2: [www.isc2.org](http://www.isc2.org)

- CISSP certification, training, awareness, community

EDUCAUSE: <http://www.educause.edu/>

- Non-profit advance higher education by promoting IT

# Podcasts

## Introductory

- Hackable?
- Smashing Security

## True Crime

- Darknet Diaries
- Malicious Life
- CPradio

## Industry News & Educational

- The CyberWire Daily
- SANS Internet Stormcenter
- Paul's Security Weekly
- Defensive Security Podcast

Information Security Office

[infosecurity@txstate.edu](mailto:infosecurity@txstate.edu)

512-245-4225