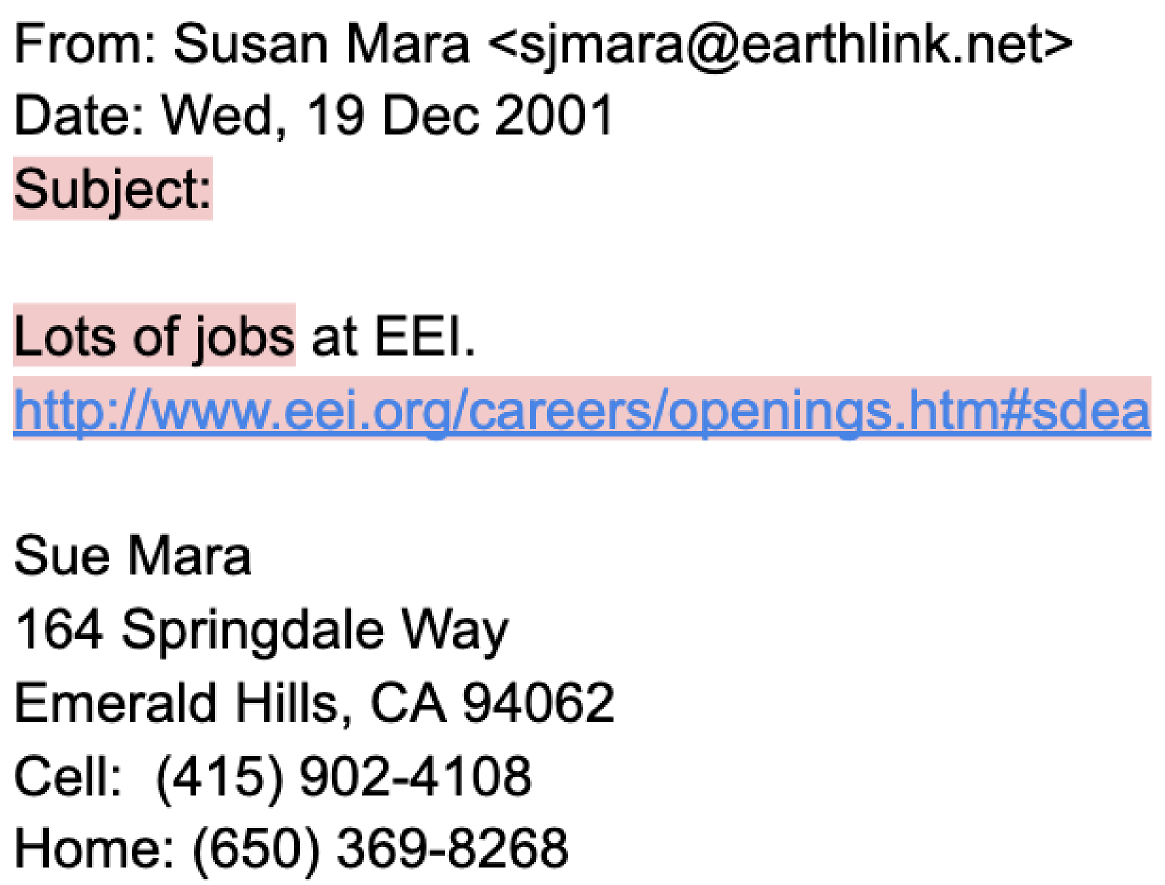
Task-2 Answer

mdfazlerabbi@isu.edu Switch account

Not shared

Email-1



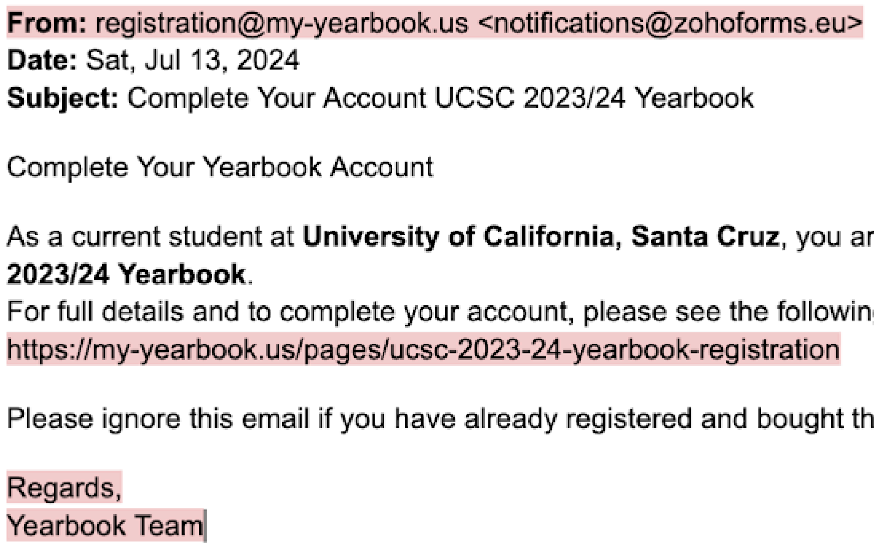
From: Susan Mara <sjmara@earthlink.net>
Date: Wed, 19 Dec 2001
Subject:

Lots of jobs at EEI.
http://www.eei.org/careers/openings.htm#sdea

Sue Mara
164 Springdale Way
Emerald Hills, CA 94062
Cell: (415) 902-4108
Home: (650) 369-8268

This is a genuine email from a specific sender with verifiable contact details. It offers job opportunities at EEI (Edison Electric Institute), and the provided link directs to a legitimate career page. The lack of urgency or requests for personal information, combined with its clear job-related purpose, confirms its authenticity.

Email-2



From: registration@my-yearbook.us <notifications@zohoforms.eu>
Date: Sat, Jul 13, 2024
Subject: Complete Your Account UCSC 2023/24 Yearbook

Complete Your Yearbook Account

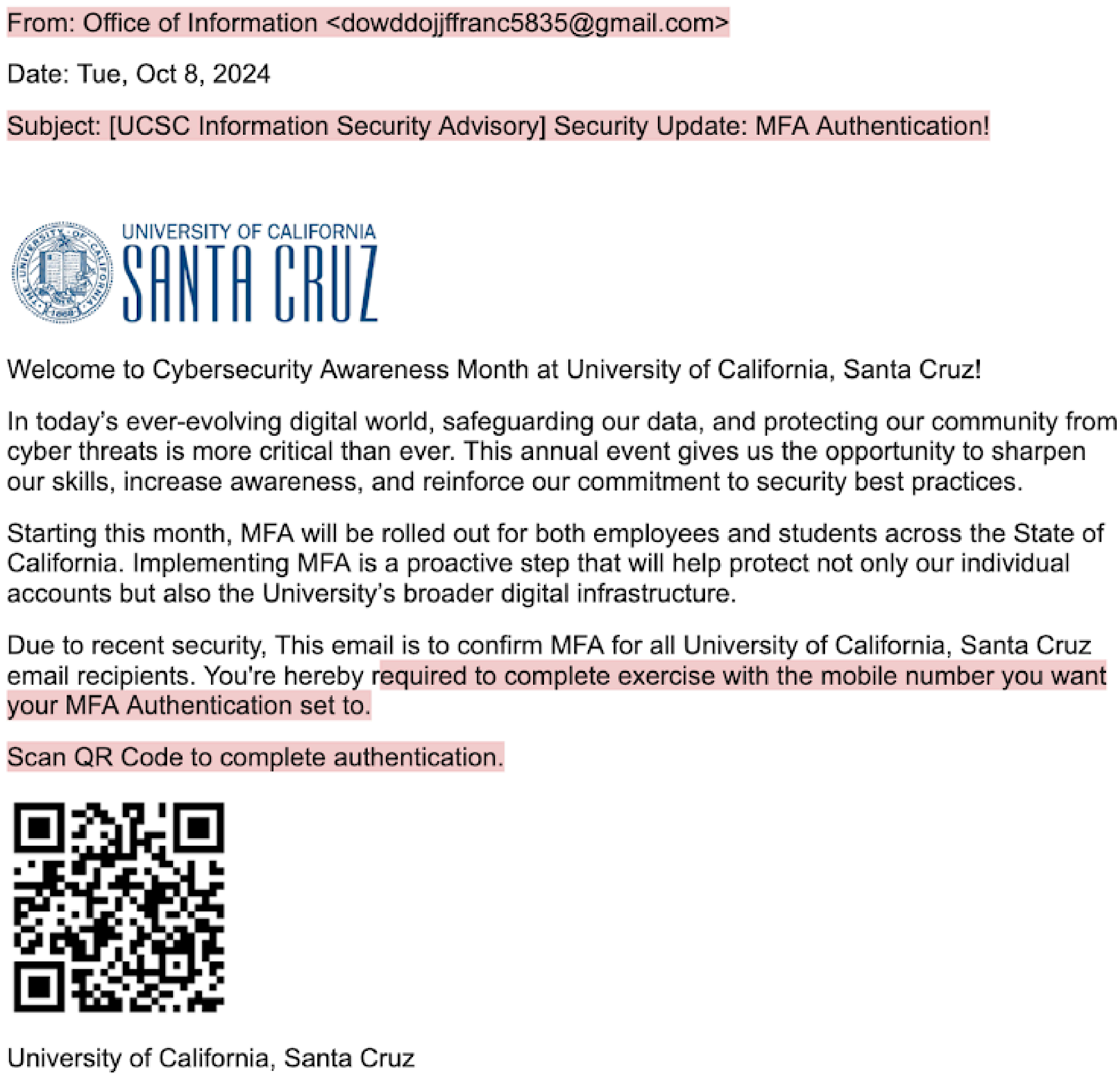
As a current student at **University of California, Santa Cruz**, you are entitled to get into our **2023/24 Yearbook**.
For full details and to complete your account, please see the following steps below:
https://my-yearbook.us/pages/ucsc-2023-24-yearbook-registration

Please ignore this email if you have already registered and bought the yearbook.

Regards,
Yearbook Team

This is a phishing email. The sender's email is not associated with an official university domain, which raises concerns about its legitimacy. Additionally, the link provided leads to an external website, which could be malicious. Phishing emails often use generic signatures like "Yearbook Team" and attempt to mimic official communications to trick recipients into clicking on fraudulent links or providing personal information.

Email-3



From: Office of Information <dowddojjffranc5835@gmail.com>

Date: Tue, Oct 8, 2024

Subject: [UCSC Information Security Advisory] Security Update: MFA Authentication!

UNIVERSITY OF CALIFORNIA
SANTA CRUZ

Welcome to Cybersecurity Awareness Month at University of California, Santa Cruz!

In today's ever-evolving digital world, safeguarding our data, and protecting our community from cyber threats is more critical than ever. This annual event gives us the opportunity to sharpen our skills, increase awareness, and reinforce our commitment to security best practices.

Starting this month, MFA will be rolled out for both employees and students across the State of California. Implementing MFA is a proactive step that will help protect not only our individual accounts but also the University's broader digital infrastructure.

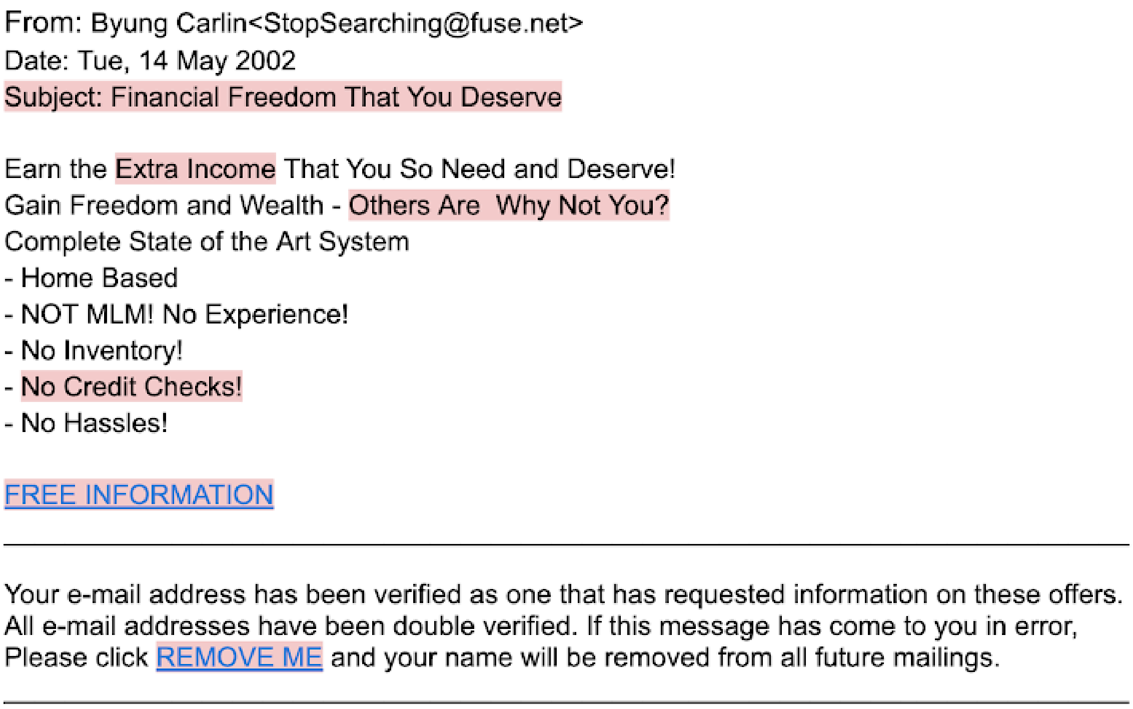
Due to recent security, This email is to confirm MFA for all University of California, Santa Cruz email recipients. You're hereby required to complete exercise with the mobile number you want your MFA Authentication set to.

Scan QR Code to complete authentication.

University of California, Santa Cruz

This email is a phishing attempt due to several suspicious signs. The sender's email is not associated with an official UCSC domain. Additionally, the email includes an urgent request to complete an MFA exercise by scanning a QR code, which is a common phishing tactic to trick recipients into providing sensitive information. The vague language, such as "complete exercise," and the emphasis on urgency are red flags.

Email-4



From: Byung Carlin<StopSearching@fuse.net>
Date: Tue, 14 May 2002
Subject: Financial Freedom That You Deserve

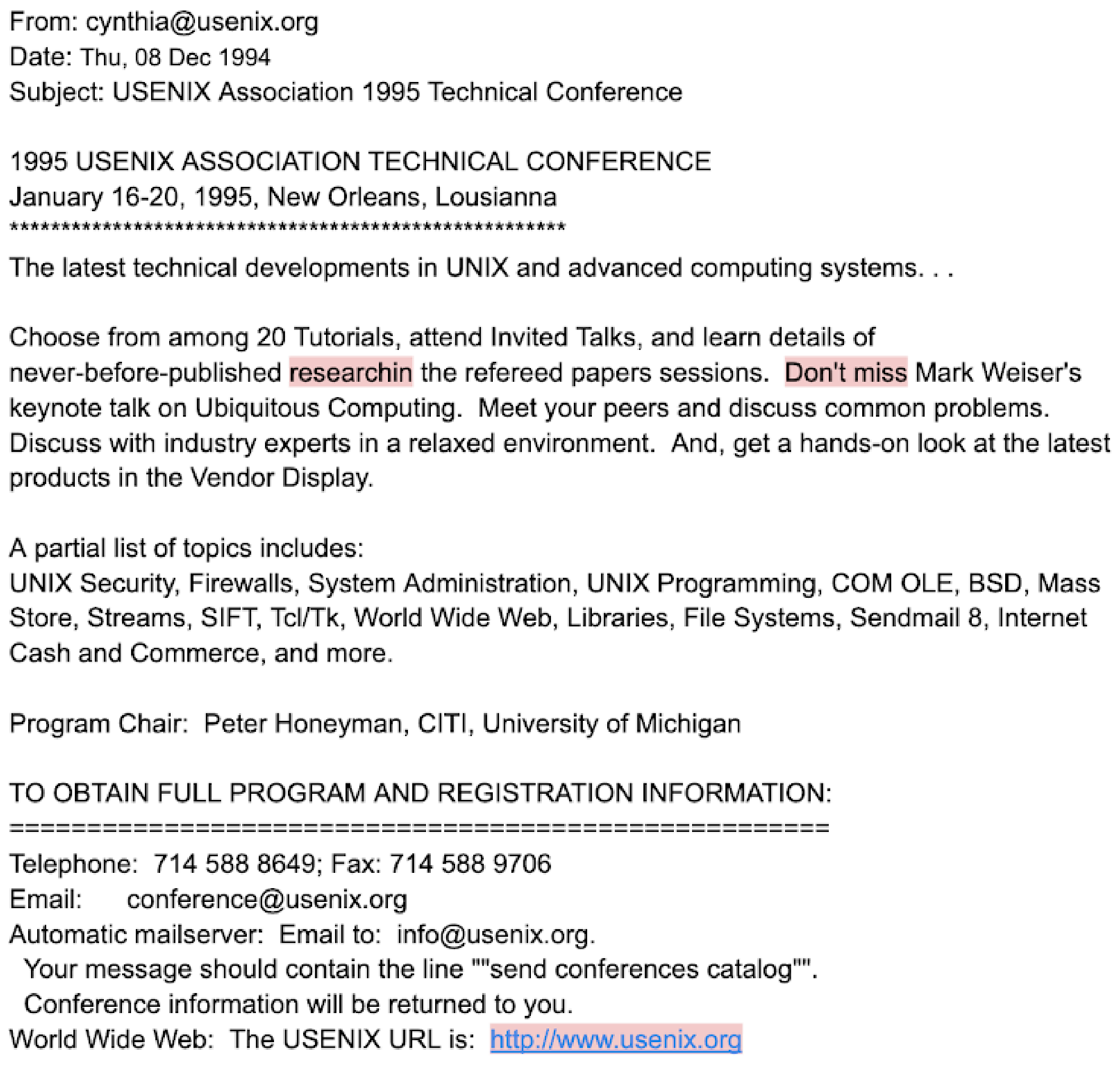
Earn the Extra Income That You So Need and Deserve!
Gain Freedom and Wealth - Others Are Why Not You?
Complete State of the Art System
- Home Based
- NOT MLM! No Experience!
- No Inventory!
- No Credit Checks!
- No Hassles!

FREE INFORMATION

Your e-mail address has been verified as one that has requested information on these offers. All e-mail addresses have been double verified. If this message has come to you in error, Please click REMOVE ME and your name will be removed from all future mailings.

This email is a phishing attempt for several reasons. The sender's email address does not match any recognizable organization, raising questions about its legitimacy. The subject, "Financial Freedom That You Deserve," and promises of unrealistic rewards with no effort are typical phishing tactics. Phrases like "Extra Income" and "No Credit Checks!" create urgency and appeal to the recipient's desire for quick financial gain. Vague claims like "Others Are Why Not You?" and suspicious links such as "FREE INFORMATION" are additional red flags designed to pressure the recipient into providing personal information without verifying the source.

Email-5



From: cynthia@usenix.org
Date: Thu, 08 Dec 1994
Subject: USENIX Association 1995 Technical Conference

1995 USENIX ASSOCIATION TECHNICAL CONFERENCE
January 16-20, 1995, New Orleans, Lousianna
****
The latest technical developments in UNIX and advanced computing systems. . .

Choose from among 20 Tutorials, attend Invited Talks, and learn details of never-before-published researchin the refereed papers sessions. Don't miss Mark Weiser's keynote talk on Ubiquitous Computing. Meet your peers and discuss common problems. Discuss with industry experts in a relaxed environment. And, get a hands-on look at the latest products in the Vendor Display.

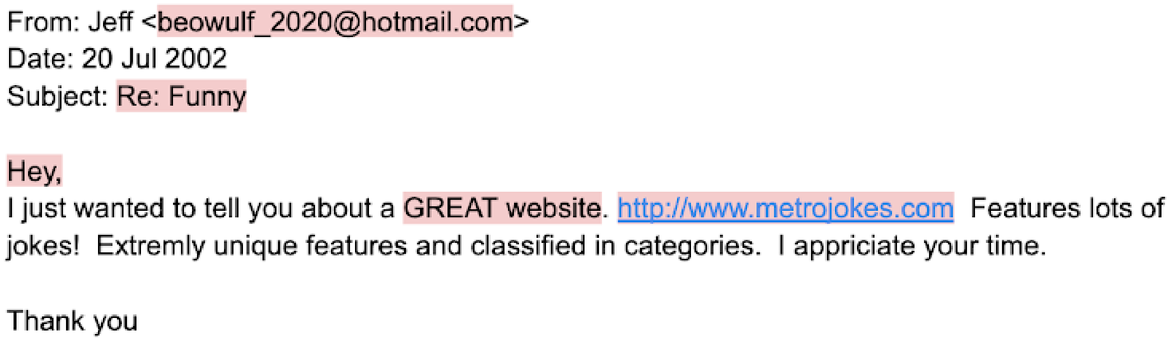
A partial list of topics includes:
UNIX Security, Firewalls, System Administration, UNIX Programming, COM OLE, BSD, Mass Store, Streams, SIFT, Tcl/Tk, World Wide Web, Libraries, File Systems, Sendmail 8, Internet Cash and Commerce, and more.

Program Chair: Peter Honeyman, CITI, University of Michigan

TO OBTAIN FULL PROGRAM AND REGISTRATION INFORMATION:
==
Telephone: 714 588 8649; Fax: 714 588 9706
Email: conference@usenix.org
Automatic mailserver: Email to: info@usenix.org.
  Your message should contain the line ""send conferences catalog"".
  Conference information will be returned to you.
World Wide Web: The USENIX URL is: http://www.usenix.org

This email is clearly legitimate. It is a formal communication from the USENIX Association about their 1995 Technical Conference. The content includes detailed information about the event which can be easily verified through the official USENIX website. There is no request for personal or financial information, and the purpose of the email is to provide valuable details about the conference, making it a trustworthy message despite the highlighted areas.

Email-6



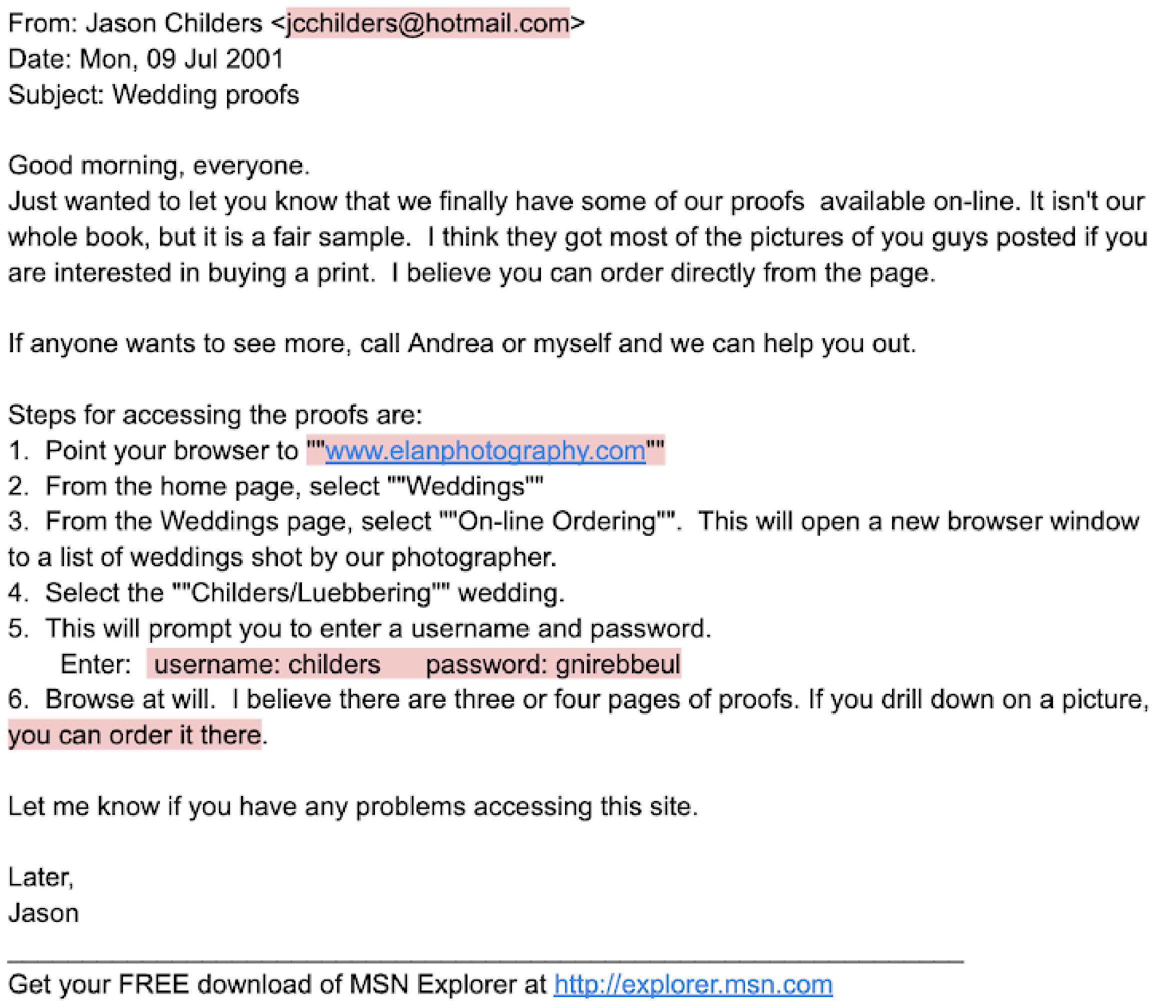
From: Jeff <beowulf_2020@hotmail.com>
Date: 20 Jul 2002
Subject: Re: Funny

Hey,
I just wanted to tell you about a GREAT website. http://www.metrojokes.com Features lots of jokes! Extremly unique features and classified in categories. I appriciate your time.

Thank you

This is a legitimate communication in which the sender is simply sharing a joke website, with no requests for personal information, urgency, or financial incentives. Although the spelling errors and informal language may raise concerns, the content and intent of the message—sharing a humorous website—indicate that it is not a phishing attempt.

Email-7



From: Jason Childers <jcchilders@hotmail.com>
Date: Mon, 09 Jul 2001
Subject: Wedding proofs

Good morning, everyone.
Just wanted to let you know that we finally have some of our proofs available on-line. It isn't our whole book, but it is a fair sample. I think they got most of the pictures of you guys posted if you are interested in buying a print. I believe you can order directly from the page.

If anyone wants to see more, call Andrea or myself and we can help you out.

Steps for accessing the proofs are:
1. Point your browser to ""www.elanphotography.com""
2. From the home page, select ""Weddings""
3. From the Weddings page, select ""On-line Ordering"". This will open a new browser window to a list of weddings shot by our photographer.
4. Select the ""Childers/Luebbering"" wedding.
5. This will prompt you to enter a username and password.
   Enter: username: childers password: gnirebbeul
6. Browse at will. I believe there are three or four pages of proofs. If you drill down on a picture, you can order it there.

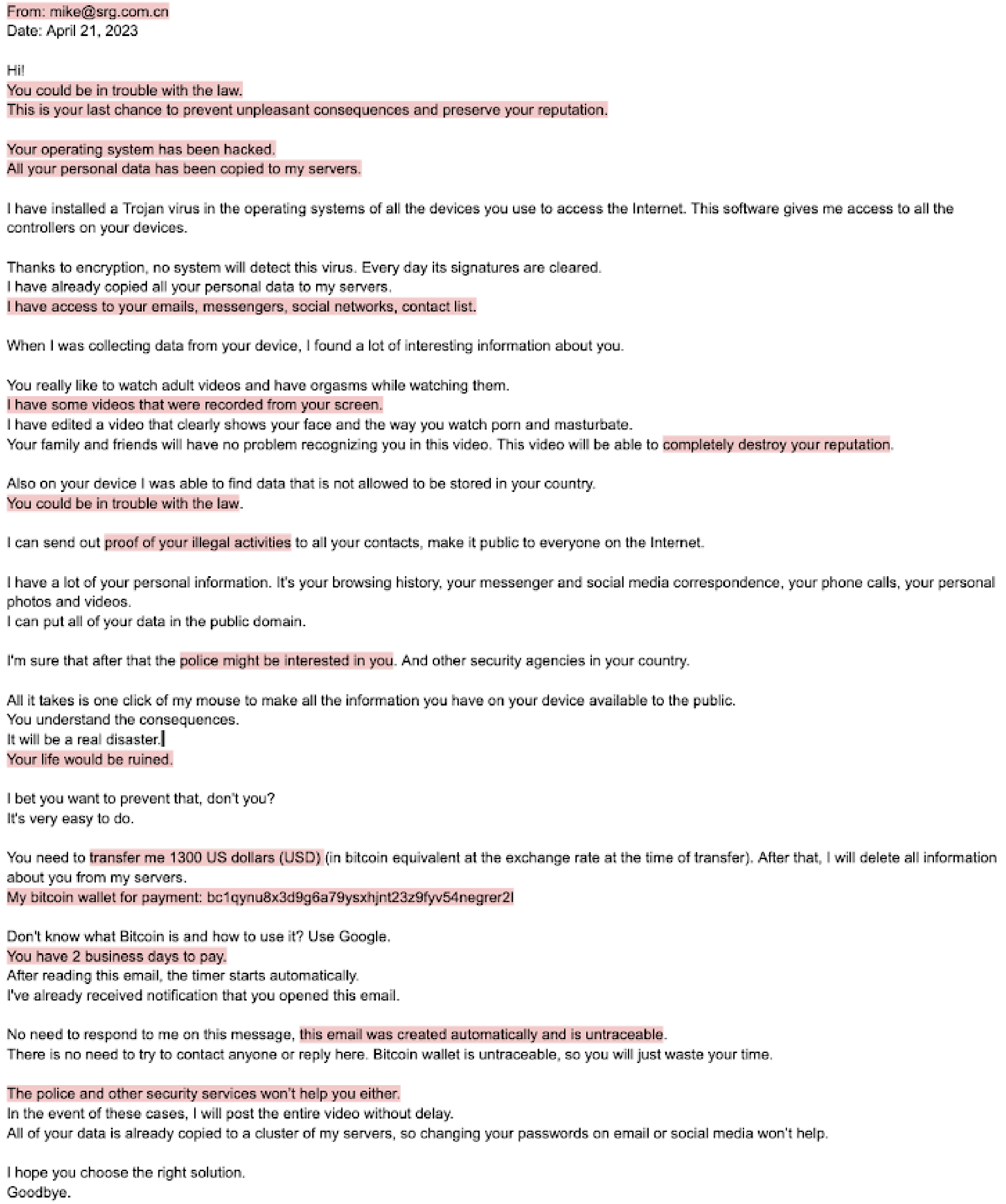
Let me know if you have any problems accessing this site.

Later,
Jason

Get your FREE download of MSN Explorer at http://explorer.msn.com

This is not a phishing email. The email context is personal and specific, related to wedding proofs that recipients are likely expecting. The instructions provided for accessing the proofs are clear and reasonable which aligns with the purpose of the message. Additionally, the sender offers direct support by inviting recipients to call if they encounter issues, showing openness and transparency.

Email-8



From: mike@srg.com.cn
Date: April 21, 2023

Hi!
You could be in trouble with the law.
This is your last chance to prevent unpleasant consequences and preserve your reputation.

Your operating system has been hacked.
All your personal data has been copied to my servers.

I have installed a Trojan virus in the operating systems of all the devices you use to access the Internet. This software gives me access to all the controllers on your devices.

Thanks to encryption, no system will detect this virus. Every day its signatures are cleared.
I have already copied all your personal data to my servers.
I have access to your emails, messengers, social networks, contact list.

When I was collecting data from your device, I found a lot of interesting information about you.

You really like to watch adult videos and have orgasms while watching them.
I have some videos that were recorded from your screen.
I have edited a video that clearly shows your face and the way you watch porn and masturbate.
Your family and friends will have no problem recognizing you in this video. This video will be able to completely destroy your reputation.

Also on your device I was able to find data that is not allowed to be stored in your country.
You could be in trouble with the law.

I can send out proof of your illegal activities to all your contacts, make it public to everyone on the Internet.

I have a lot of your personal information. It's your browsing history, your messenger and social media correspondence, your phone calls, your personal photos and videos.
I can put all of your data in the public domain.

I'm sure that after that the police might be interested in you. And other security agencies in your country.

All it takes is one click of my mouse to make all the information you have on your device available to the public.
You understand the consequences.
It will be a real disaster.
Your life would be ruined.

I bet you want to prevent that, don't you?
It's very easy to do.

You need to transfer me 1300 US dollars (USD) (in bitcoin equivalent at the exchange rate at the time of transfer). After that, I will delete all information about you from my servers.
My bitcoin wallet for payment: bc1qynu8x3d9g6a79ysxhjnt23z9fyv54negrer2l

Don't know what Bitcoin is and how to use it? Use Google.
You have 2 business days to pay.
After reading this email, the timer starts automatically.
I've already received notification that you opened this email.

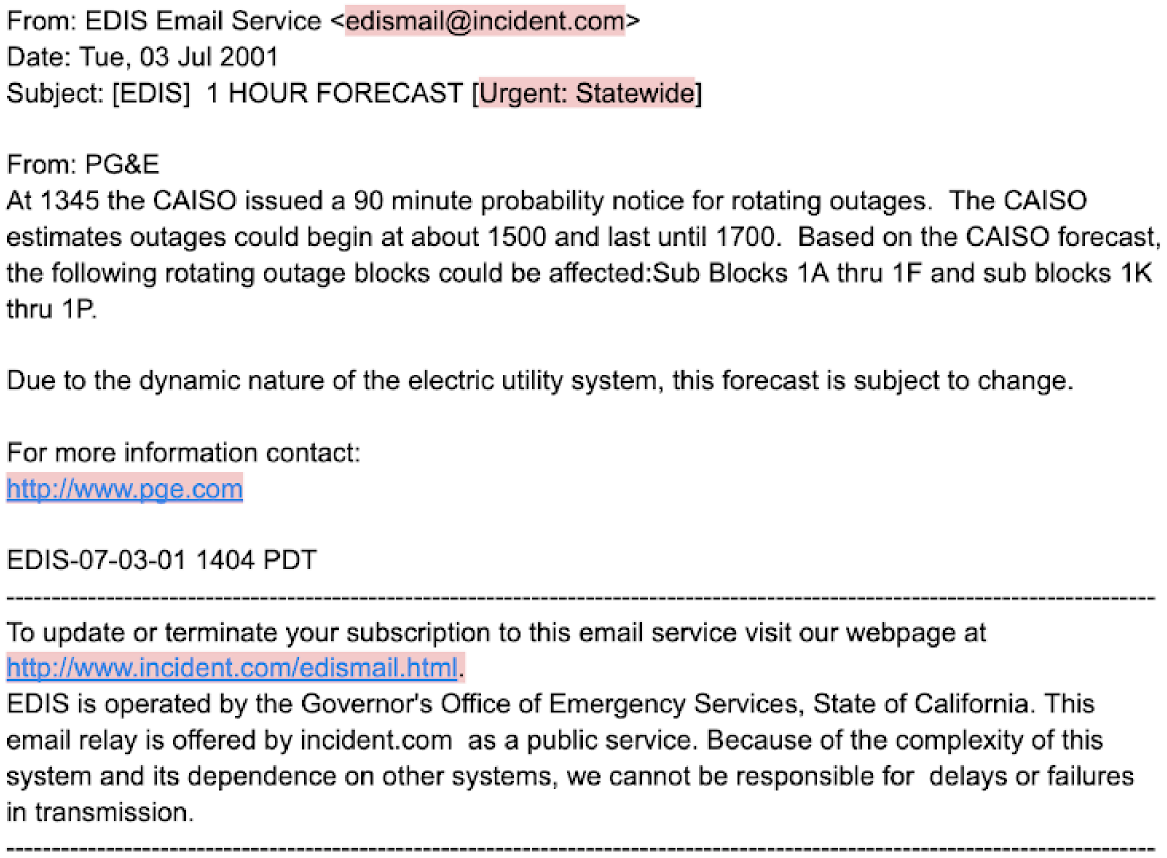
No need to respond to me on this message, this email was created automatically and is untraceable.
There is no need to try to contact anyone or reply here. Bitcoin wallet is untraceable, so you will just waste your time.

The police and other security services won't help you either.
In the event of these cases, I will post the entire video without delay.
All of your data is already copied to a cluster of my servers, so changing your passwords on email or social media won't help.

I hope you choose the right solution.
Goodbye.

This email is a phishing attempt designed to scare the recipient into paying 1300 USD in Bitcoin by falsely claiming their system has been hacked and sensitive data stolen. It uses threats of exposing personal information and ruining the recipient's reputation if payment isn't made, which is a common tactic in extortion scams. The suspicious email address and vague threats further indicate it's a scam.

Email-9



From: EDIS Email Service <edismail@incident.com>
Date: Tue, 03 Jul 2001
Subject: [EDIS] 1 HOUR FORECAST [Urgent: Statewide]

From: PG&E
At 1345 the CAISO issued a 90 minute probability notice for rotating outages. The CAISO estimates outages could begin at about 1500 and last until 1700. Based on the CAISO forecast, the following rotating outage blocks could be affected:Sub Blocks 1A thru 1F and sub blocks 1K thru 1P.

Due to the dynamic nature of the electric utility system, this forecast is subject to change.

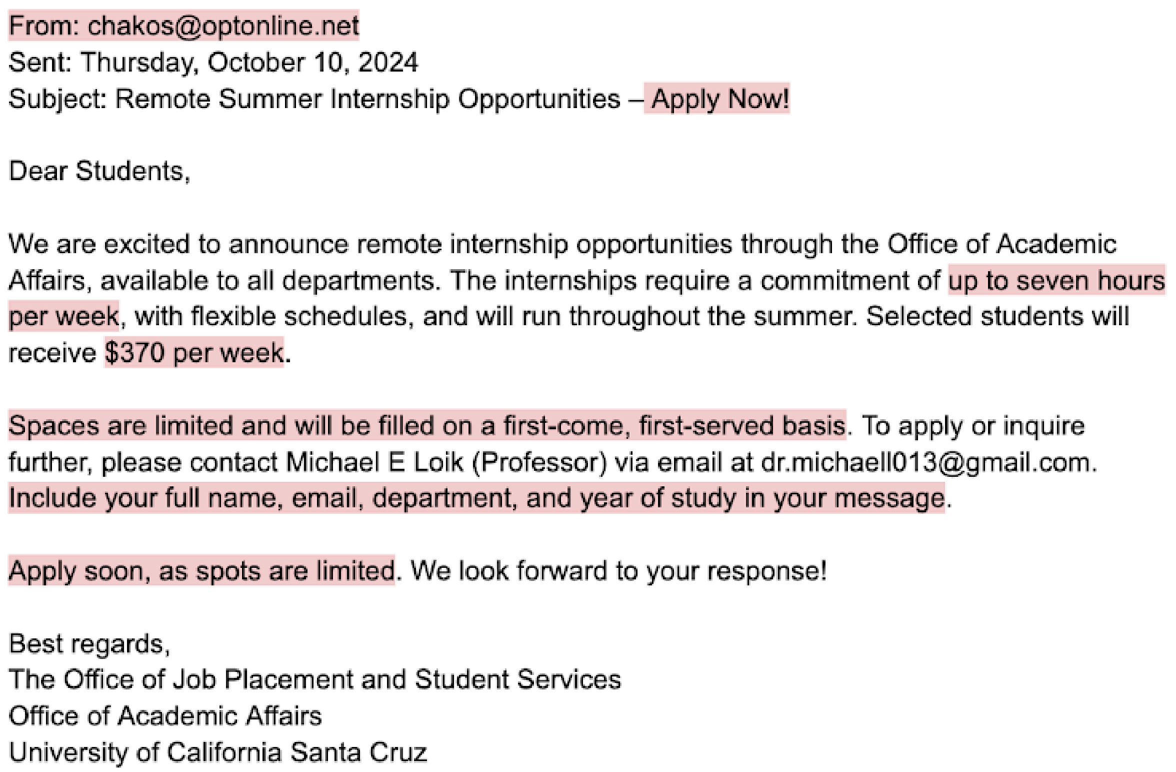
For more information contact:
http://www.pge.com

EDIS-07-03-01 1404 PDT

To update or terminate your subscription to this email service visit our webpage at http://www.incident.com/edismail.html.
EDIS is operated by the Governor's Office of Emergency Services, State of California. This email relay is offered by incident.com as a public service. Because of the complexity of this system and its dependence on other systems, we cannot be responsible for delays or failures in transmission.

This is a legitimate email sent from a recognizable service, EDIS (Emergency Digital Information Service), providing important details about potential power outages. It includes a clear explanation of the issue, the time window for the outage, and links to authentic official websites such as PG&E. Additionally, the message contains standard subscription management options and is signed off with details about the California Governor's Office of Emergency Services, further supporting its legitimacy.

Email-10



From: chakos@optonline.net
Sent: Thursday, October 10, 2024
Subject: Remote Summer Internship Opportunities – Apply Now!

Dear Students,

We are excited to announce remote internship opportunities through the Office of Academic Affairs, available to all departments. The internships require a commitment of up to seven hours per week, with flexible schedules, and will run throughout the summer. Selected students will receive $370 per week.

Spaces are limited and will be filled on a first-come, first-served basis. To apply or inquire further, please contact Michael E Loik (Professor) via email at dr.michaell013@gmail.com. Include your full name, email, department, and year of study in your message.

Apply soon, as spots are limited. We look forward to your response!

Best regards,
The Office of Job Placement and Student Services
Office of Academic Affairs
University of California Santa Cruz

This email is a phishing attempt with several red flags. The sender's email is not from an official university domain, and a personal Gmail address is used for contact, both raising doubts. Urgency phrases like "Apply Now!," "Spaces are limited," and promises of specific pay without verification are common phishing tactics to pressure recipients into providing personal information.

Submit

Clear form

Never submit passwords through Google Forms.