How to Protect Yourself from Phishing

By: Eric Gonzalez

Agenda

01 **What is Phishing?**

02 **What Does Phishing Look Like?**

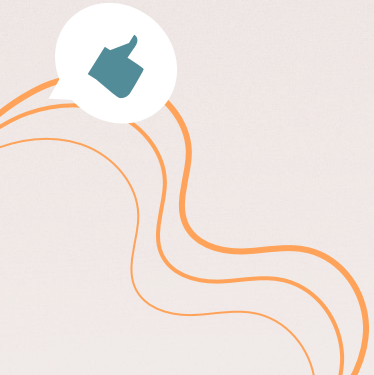**03** **How to Protect Against Phishing**

04 **Reminders and Tips for Staying Safe**

01

What is Phishing?

What is Phishing?

Phishing is pretending to be someone in order to get access to private information. This is often done through sending scam emails designed to get people to click on a link or share privileged information.

Attackers are often looking for critical information such as passwords and other login info, which ends up costing companies millions of dollars in damages.

02

What Does Phishing Look Like?

Learn How to Spot Phishing Emails

Here are a few indicators of phishing emails:

- Incomplete sentences/bad grammar

- Incorrect email headers

- Embedded links that hide the url

- A sense of urgency and immediate action requested

- Sounds "too good to be true"

Ready to Practice?

What Sticks Out In This Email?

Internship Opportunity at UCSC `External` `Inbox ×`

Nitin Goswami <safferc@optimum.net>
to ▾

Dear Students,

The Office of Job Placement and Student Services at the University of California, Santa Cruz is pleased to announce a selection of exclusive internship opportunities, including remote positions. These internships provide invaluable, hands-on research experience while offering financial compensation. Interns are expected to commit up to seven hours per week and will receive a competitive weekly stipend of $475.

We encourage applications from both undergraduate and graduate students across all academic disciplines. This is a unique opportunity to enhance your skill set, expand your professional network, and gain practical, career-relevant experience. Please note that positions are limited and will be filled on a first-come, first-served basis.

To apply, please submit the following information to Prof. Eric Porter at Ecpporter@gmail.com:

Full Name

Alternate Email Address

Phone Number

Academic Department

Year of Study

We look forward to reviewing your application and supporting your academic and professional development.

Best regards,
Office of Job Placement and Student Services
University of California, Santa Cruz.

↩ Reply   → Forward

What Sticks Out In This Email?

Internship Opportunity at UCSC `External` `Inbox ×`

Nitin Goswam `<safferc@optimum.net>`
to ▾

Email addresses not from UCSC school domain of "@ucsc.edu"

Lack of first name personalization

Dear Students,

The Office of Job Placement and Student Services at the University of California, Santa Cruz is pleased to announce a selection of exclusive internship opportunities, including remote positions. These internships provide invaluable, hands-on research experience while offering financial compensation. Interns are expected to commit up to seven hours per week and will receive a competitive weekly stipend of $475.

Too good to be true

We encourage applications from both undergraduate and graduate students across all academic disciplines. This is a unique opportunity to enhance your skill set, expand your professional network, and gain practical, career-relevant experience. Please note that positions are limited and will be filled on a first-come, first-served basis.

To apply, please submit the following information to Prof. Eric Porter at Ecpporter@gmail.com:

Full Name

Alternate Email Address

Phone Number

Academic Department

Year of Study

Requesting personal information

Sense of urgency

We look forward to reviewing your application and supporting your academic and professional development.

Best regards,
Office of Job Placement and Student Services
University of California, Santa Cruz.

↩ Reply   → Forward

03

# How to Protect Yourself Against Phishing
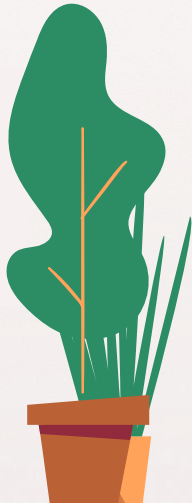
Protect Against Phishing Emails

- Look at who sent the email. Can you verify that they are a part of your organization, such as by checking the company website or asking other employees?

- Look out for incomplete sentences and bad grammar, as they are often common indicators that the email is counterfeit

- Contact your official IT department if you have any doubts about an email's legitimacy

04

Reminders and Tips for Staying Safe
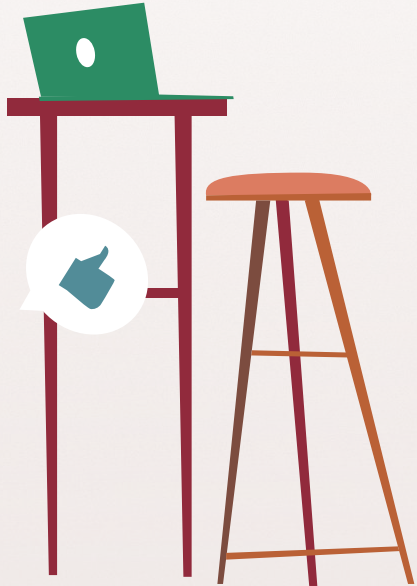
Remember to always...

- Verify the source of the email

- Be suspicious of emails asking for your personal information

- Check the source of any hyperlinks

- Look out for other signs of phishing emails, such as a sense of urgency or an offer that sounds too good to be true

- Reach out to your IT department if you think an email looks suspicious

- Be cautious! It is better to be safe than sorry!