Lake-Sumter State College

6 Red Flags That Suggest a Potential Phishing Attempt

1. Is the email from a free account or spoofed email account?

Is The Email From a Legitimate Email Address?

Be wary of recruiters using free web email accounts from services like Gmail or Hotmail instead of using a business email address to contact you. There may be tell-tale signs within the email itself, too. While some scammers may send out well-written emails, many will seem unprofessional. If the email contains excessive spelling or punctuation mistakes, incorrect capitalization, or grammatical errors, it could be from a fake recruiter.

Examples

- lakesumterstate@hotmail.com
- lakesumtersc2021@gmail.com

Is the Source Trustworthy?

Emails may appear to come from a trustworthy source, even from someone from within the same email domain. However, when you click to reply to the email, you will see a different recipient name in the 'To:' box. Please double-check to verify that the intended recipient matches the original sender's name and uses a business email address.

Please note that this is similar to hackers that spoof/impersonate phone numbers within the same area code and prefix (vishing). You may be more likely to answer such a call since you may believe that the caller is nearby. Please be vigilant!

Example

A user may receive an email that appears to come from Someone@student.lssc.edu, but the reply address would actually take you to BogusEmail@hotmail.com.

Have You Screened the Email's Attachments?

It's also important to consider attachments sent in emails. If you are unsure about the legitimacy of the file, use a virus scanner before opening it. Some scammers may send attachments that contain viruses designed to corrupt your device and extract personal information.

2. Are they asking for money or unnecessary personal information before submitting your application?

While discussing job opportunities, you should not be asked for payment before being submitted. Some scammers might ask you to set up a new bank account and give them the details or send you to a website and fill out a credit report form. In these instances, the scammer might say that they need your details to

put you onto the company insurance. Please fiercely guard your personal banking, credit card, and online payment information. Genuine recruiters may ask for your contact details, an up-to-date resume, references, and salary expectations. However, they should always be open and honest about why they need these details. They should never ask you to transfer any money before starting the recruitment process. You should never give out your full Social Security Number or date of birth before successfully securing a new position and beginning the onboarding process.

Stay vigilant on the request of the following information:

- Payment before submitting an application
- Bank account details
- Credit card and online payment information
- Request to transfer money
- Social Security Number

Online forms

If a "recruiter" asks you to fill out a form, always check that the website they send you to is secure. You can do this by looking at the web address bar. If the address is HTTP:// then it isn't secure; only HTTPS:// sites are secure.

3. Is the recruiter being evasive when asked about the job in question?

Recruiters should always be knowledgeable about the job they're recommending. If they seem vague, fail to answer your questions correctly, or gloss over the finer details, this should set off alarm bells. If they cannot answer your questions satisfactorily, it's a sign that they might not be who they say they are. That said, sometimes genuine recruiters have a confidential role and can't disclose the client's name. Nevertheless, they should still know the industry and will disclose as much information about the role as they can.

Example of A Good Response :

Please check our website so you can learn about our wonderful business and view testimonials from our staff. Please also check out information about our current projects and plans moving forward. I will include you in an email to your supervisor who is our CIO so you can get even more details about your day-to-day obligations directly.

Example of A Bdd Response:

I am currently out of the country and in Australia starting up a new business. You will only work 3 hours a week doing some clerical work and be paid $500 in advance. Since this is a new business you'll also represent me in business processes in the US until I return.

4. Does this job offers sound too good to be true?

Scammers will make their job offers as appealing as possible to entice people to share information with them. Be on your guard if they present a job opportunity that seems too good to be true. While most job descriptions highlight the benefits of a role, fake descriptions may have an abnormally long list. They may also say 'no experience necessary and have shorter hours than expected of the role in question.

5. Are they instantly offering a high salary?

Similar to the point above, fake job offers tend to include unrealistically high salaries. For example, a starting job salary 50-100% above the average rate is unlikely to be real.

If the salary offered seems at odds with the job role, it's worth questioning whether the job is part of a scam.

6. Are they offering you the job without an interview?

Some scammers may even offer you the job without even putting you through for an interview. Some will go further and have an interview with you on the phone, but this won't be with the company' hiring'; you'll just speak to the fake recruiter. Another tactic scammers use is to invite you to an online job interview using an unfamiliar or insecure messaging service. Scammers can obtain your details by asking you to set up an account on the online chat platform. It is recommended that you research any software or websites you are invited to sign up to.

Part of a genuine recruiter's job is to spend time ensuring you're the right fit for the company that's hiring. If they offer you the role without even putting you through for an interview, the chances are it's a scam.

It might seem scary that people would go to these lengths to scam somebody, but luckily, there are several ways to check whether a recruitment agency is genuine. Regardless of whether a recruiter is legitimate or not, it would be best if you always asked questions when discussing a role. However, this is especially important if you suspect the person you're talking to is a scammer.

Examples of good questions to ask a recruitment agency/hiring manager:

- Have you placed any previous candidates with your client?
- What can you tell me about the company's culture?
- What opportunities are there for growth in this role?
- Please can you tell me more about the role?
- How long has the company been operating?

Add these steps to your verification process.

- Legitimate agencies and hiring managers always invest time and effort into the recruitment process. Even if the role is confidential, they should be able to answer the majority of your questions.
- Check their LinkedIn profile. If you get contacted by a recruiter, your first port of call should always be LinkedIn. If their profile doesn't have a lot of connections or has incomplete information, this could be a warning sign.
- Please make sure the recruiter's LinkedIn profile is connected to their agency's corporate page. If it isn't, this could suggest that they don't really work for an official firm.
- If the recruiter or hiring manager claims to be affiliated with Lake-Sumter State College, please verify their employment with our HR department and by using our online website online: https://www.lssc.edu/directory/
- Copy the recruiter's profile photo and text from their bio and paste it into a Google Search. Scammers often steal information from real recruiters to create their own illegitimate profiles.