THE UNIVERSITY OF CHICAGO

security@uchicago.edu

How to Identify a Phishing Scam

Can you recognize a phishing scam?

Read on for tips to help you foil a phisherman! You can look at examples of different kinds of phishing emails at our Phishing Examples page. You can also look at the database at antiphishing.org to see examples of many different phishing scams reported throughout the year.

This message looks funny...

If you are not sure an email is legitimate, ask yourself these questions before replying or clicking a link. Keep in mind that University administrators and IT Services personnel *will never request your CNetID username or password by email*. If an email claims to be from the University, IT Services, or the uchicago.edu team and asks you to reply with private information, it is a scam.

First, check the header…

Have I given my email address to this company before? Do I have an account with this company? Does the sender identity match the purpose of email?

Any communication from a bank, health provider, or other legitimate company with which you do business, should come from that organization's email system, not from some unrelated email address. For example, an email from the University should come from an address like

sender@uchicago.edu, not from *sender@uchicago.com* or *sender@maildrop.cc*.
If you do not have a relationship with the sender, or the email address is inconsistent with the identity of the sender, 99% of the time it is a phishing email.

- Is my email listed as the **From:** address? If so, it is not a legitimate email
- Is the **To:** address to *undisclosed-recipients* or to a large number of recipients you are not familiar with?

A legitimate email from an organization you do have business with will usually be addressed only to you. If the text alludes to confidential information but has several addresses on the **To:** line, it is definitely not legitimate.

Check the content

Do links provided in the body of the email look valid?
Make it a habit to check all links *before* you click them. Even though it might look correct in the text, *it could take you someplace completely different*. Don't ever click a link or an image without verifying that the link is legitimate; you could be redirected to an attacker's website.

Rest, but *do not click* the mouse pointer on the link, and check the location displayed in the bottom left corner of your browser screen to verify the real location. Watch out for web addresses that resemble the name of a well-known company, but are slightly altered by adding, omitting, or transposing letters. For example, the common address `www.microsoft.com` could appear instead as one of the following:

```
http://www.micosoft.com
http://www.mircosoft.com
http://www.verify-microsoft.com
```

Are there misspelling and typos? How is the grammar and is the tone appropriate?

An email from a professional company should be well written.

Am I being promised a lot of money for little or no effort on my part?

Watch out for emails with claims like:

- "You have won the lottery" (perhaps one from a foreign country) that you don't remember entering.
- A foreign government official would like your assistance in transferring funds and will pay you a hefty commission if you agree
- You stand to inherit millions of dollars from a relative you did not know you had.

These are common phishing scams known as advanced fee fraud. Remember that if it sounds too good to be true, it probably is too good to be true.

Am I asked to provide money up front for questionable activities, a processing fee, or to pay the cost of expediting the process?

This is a common way for con artists to scam money from unsuspecting users. The con artist will run away after taking your initial payment.

Is someone asking me for my bank account number, other personal financial information or passwords?

Beware of emails asking for this information, even if the sender offers to deposit money into your account. Be suspicious of phrases like:

- "Verify your account."
- "Click the link below to gain access to your account."

Consider the purpose of the email

Email is *not* a secure way to share sensitive information. Businesses should not ask you to send passwords, login names, social security numbers, or other personal information through email.

Is the issue really as urgent as the sender makes it out to be?

Con artists try to convey a sense of urgency so that you'll respond immediately without thinking. Be suspicious of phrases like:

- If you don't respond within 48 hours, your account will be closed
- Failure to do this may automatically render your account deactivated.
- Our investigation shows that your email address is compromised and is used to send out spam message in our webmail system. As a result, our network engineer will be conducting a maintenance in our webmail system, your Username will be disabled if you do not send us the required information within 48 hrs.

Why does the sender request confidentiality? How can I tell if evidence that the proposed activity is legitimate and really authentic?

Be suspicious about offers to send you photocopies of government certificates, banking information, or other evidence that their activity is legitimate. Photocopies are not acceptable for verifying the authenticity of documents. These are often fake.

Be cautious about opening attachments

One of the most common methods for spreading computer viruses and other malicious software is through email attachments. When opened, these attachments can give someone else complete control of your machine, initiate attacks on other machines, or start spamming every contact it finds in your address book. Malevolent software (malware) of this type has crippled personal machines, email servers, and networks at many companies.

Here are a few simple guidelines to ward off malicious attachments:

- Do not open unexpected attachments. If you don't open or view an attachment, you are at far less risk. Many people fall into the habit of opening attachments without thinking about it. **Don't do this**! You should always think about whether you want to open the attachment first. Assume an attachment is hostile. If you do know the person in question, but were not expecting them to send you an attachment, contact them and confirm that they sent it before you open it
- Do not open attachments from strangers. Always be absolutely certain you know the sender first.
- Do not open unusual attachments. Most attachments you receive are probably just documents such as Word files, Excel spreadsheets, PowerPoint presentations, or Acrobat PDFs. Learn to recognize the icons and filename extensions associated with these files. If you receive an attachment that has an unusual icon or an unusual extension, especially ones like `.pif`, `.scr`, or `.exe`, do not open it.
- Don't open attachments that come with strange-looking messages. If you receive several unexpected messages from different people with identical subject lines, it could be a virus or worm. If the subject line or message body before the attachment seems unusually vague, incoherent, or incomplete, don't open the attachment. If it just looks "wrong," don't open the attachment.