



LEGAL ALERT

www.swlaw.com

November 2007

SNELL & WILMER

Snell & Wilmer has been providing exceptional service to clients since 1938. With more than 400 attorneys in offices throughout the Western United States, we are one of the largest, most respected full-service law firms in the region. Our diverse client base consists of large, publicly traded corporations, small businesses, emerging organizations, individuals and entrepreneurs. We have the experience and ability to address virtually any legal matter for both businesses and individuals. Over the years, Snell & Wilmer has earned a reputation for distinguished service by offering our clients what they value--exceptional legal skills, quick response and practical solutions with the highest level of professional integrity.

Snell & Wilmer
L.L.P.
LAW OFFICES

DON'T GET HOOKED BY "EEOC" PHISHING EMAIL

Human resource professionals have been receiving emails from the Equal Employment Opportunity Commission ("EEOC"). But these emails are not from the EEOC: they are phony, "phishing" emails. A phishing email is an email received from what appears to be a business or organization with whom the recipient has done, or likely would do, business. The email is not actually from that business, however, but is instead a scam. The email often requests personal information or asks the recipient to follow a link or download an attached file, which may contain a computer virus.

The recent EEOC phishing email titled "Harassment Complaint Update For" purports to be from the EEOC, and even contains the EEOC logo. It claims to be an update on a harassment complaint and provides a link or attachment where the recipient can go to view an update on the alleged complaint. Following the link or downloading the attachment, however, may download a Trojan Horse worm or virus.

How To Avoid This And Other Phishing Email Scams

There are many tips to avoid falling for this or any other email scams.

- Analyze the grammar and syntax in the email. For example, the subject of this EEOC email ends in a preposition: "Harassment Complaint Update For." If the grammar or syntax seem "off," the email may be a hoax.
- Determine if the email is out of the ordinary. Our experience with the EEOC is that it rarely communicates by email and it NEVER gives updates on investigations, whether by email or regular "snail" mail. If an email seems out of the ordinary, be cautious when opening it, and do not open any attachments or internal links provided.



- Examine the sender's email address. Is it exactly as you would expect for that business or organization, or is the address only close? If it is only close, delete the email and do not open any attachments or click on any internal links.
- Do not follow any links contained in an email you suspect may be questionable. If you think the email may be legitimate, manually type the link you already have for the business instead of cutting and pasting the one provided, or clicking on the link.
- Always be highly cautious when opening any email attachments. Be sure that you know the sender and you have been previously informed of the contents of the attachment.
- Do not provide personal information in an email. Legitimate companies do not ask for personal information, such as social security numbers or bank account information, via email.
- Do not believe that an email is credible just because it provides a local phone number. Internet scammers will often use Voice Over Internet Protocol technology which enables them to choose any area code, regardless of their actual location. If you question whether the email may be legitimate, call the number that you already have for the organization or business, not the one provided in the email.
- Delete emails asking for donations or investments.
- Use and also update anti-spyware and firewall software regularly.

- When in doubt, check the legitimate company or organization's website for any warnings about phishing or other dubious emails purportedly from the company. Often times, these warnings are on the home page of the company or organization, as is the case with this EEOC phishing email.

If you receive a phishing email, forward it to the company from which the email purported to come. If you have been or end up being scammed, file a complaint at www.ftc.gov.

If you have any additional questions or are interested in learning more about this, or any other email you receive that seems suspect, please feel free to contact us.

William R. Hayden
602.382.6329 | bhayden@swlaw.com

Nathan J. Kunz
602.382.6346 | nkunz@swlaw.com

Sample Email

FROM: Equal Employment Opportunity Commission

SUBJECT: "Harassment Complaint Update For"

This is an automated email that confirms the registration of harassment complaint #number ... this harassment complaint can lead to law enforcement action. You can download and print a copy of this complaint to keep for your personal records here. ... Our staff will keep you updated regarding the status of our investigation. ... To check the status of your complaint access: