Phishing | Malicious emails and messages pretending to be from ISHR

23.06.2021

The International Service for Human Rights is warning that phishing emails, camouflaged to appear as sent by an organisation called International Society for Human Rights and using the same acronym ISHR, are being disseminated with the goal of delivering malware and stealing information under the pretext of an invitation to an *"International Human Right Conference on (Elimination Violence Against Women & Children, Human Trafficking and Child Abuse) Taking place from the 21st - 24th of JUNE 2021 in Massachusetts , Boston the United States and from the 27th - 30th of JUNE 2021 in Saint Louis, Senegal.*

These events are NOT organised by the International Service for Human Rights and we have no relation whatsoever with the organisers.

If you receive an email that you suspect to be a phishing attempt under ISHR name or if you are unsure of an email's legitimacy, please do not respond, do not click any link and do not download any file from this email on your computer.

Recommendations:

1. If you are contacted by a person or organisation that appears to be the International Society for Human Rights (ISHR), verify their authenticity before responding.
2. Verify the sender's email address. Any email address other than '@ishr.ch' format is not from us - the International Service for Human Rights (ISHR). For example, ISHR does not control email addresses ending in @usa.com
3. Check the link, before you click. Make sure the links start with https://www.ishr.ch
4. Don't provide your personal information, if you have any concerns.

What is a Phishing Attack?

> A phishing attack is a scam and an effort to steal your personal information. Phishing attacks typically come in the form of fraudulent email messages that appear to have come from a legitimate source, such as your university or bank. Phishing emails will usually direct to a spoofed website or trick the receiver into divulging personal information like account passwords, credit card information, etc.
>
> These attacks are often designed to appear urgent and panic recipients so that they take immediate action before verifying the legitimacy of the claim made. For example, a phishing email may claim the receiver will lose their account if they do not reset their password immediately through a provided link. Such claims are always indicative of a phishing scam as responsible companies and organizations would never take these actions via email.
>
> If you receive a phishing email, it does not mean your account was hacked. All a phisher needs is your email address, and they can easily send you a fraudulent and misleading email. Education and awareness are the keys to protecting yourself and your private information. - UCONN University of Connecticut

Image: ISHR/Canva