

ALLARME PHISHING "PRO TERREMOTO HAITI"

In questi giorni sono stati posti in circolazione diversi messaggi di phishing che, invitando ad effettuare una donazione "pro terremotati Haiti", tentano di carpire i dati personali per l'accesso ai conti correnti on line degli utenti.



Posteitaliane

Gentile utente,

Un forte terremoto ha colpito Haiti, causando moltissime vittime e migliaia di feriti. Il terremoto, di magnitudo 7 gradi Richter, ha causato ampi danni nella capitale Port-au-Prince e nei dintorni, lasciando molte persone senza un tetto.

C'è bisogno di cibo per evitare che la fame aggravi ancor di più le condizioni già terribili di chi è stato colpito dal disastro.

Si tratta del peggiore terremoto che colpisce Haiti negli ultimi duecento anni. L'assistenza alimentare d'emergenza costituisce una parte essenziale della risposta internazionale al disastro.

Il WFP ha subito attivato le sue procedure d'emergenza, come la distribuzione di biscotti ad alto contenuto energetico e altra assistenza alimentare alle persone colpite.

Aiutaci a raggiungere chi ha bisogno. Dona ora.

Puoi donare online 1 (uno) Eur

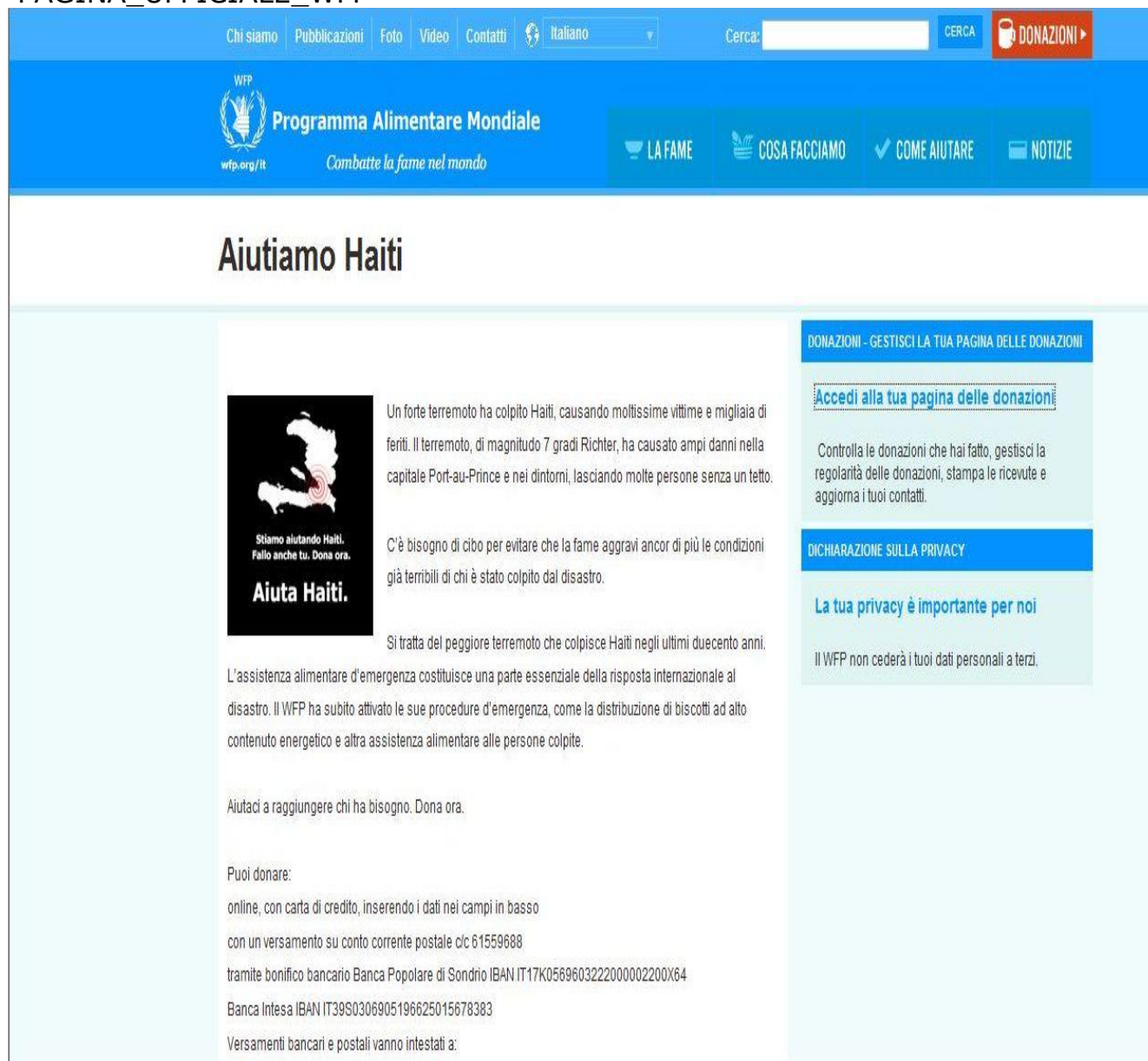
[Accedi ai servizi online per accreditate donazione](#)

L'e-mail in questione reca il logo della Croce Rossa e di Poste Italiane e, dopo aver presentato brevemente la drammatica situazione di Haiti a seguito del grave sisma (citando, fra l'altro, anche il WFP, il Programma Alimentare Mondiale delle Nazioni Unite) invita i destinatari a cliccare su un link che reindirizza l'utente ad un sito che consente di effettuare una donazione tramite conto corrente on line.

Ovviamente l'unico scopo di questa attività fraudolenta è quello di far leva sui sentimenti provati nei confronti delle popolazioni colpite dal gravissimo terremoto per carpire i codici di accesso al conto corrente on line delle vittime per utilizzarli a scopi criminosi.

Gli accertamenti della Polizia Postale di Pescara hanno fatto emergere che la mail ricalca fedelmente nel testo la pagina ufficiale del WFP (allegata alla presente a titolo di esempio) e che sia la falsa mail che la pagina per le false donazioni riconducono a provider esteri che sono oggetto di indagine.

PAGINA_UFFICIALE_WFP



The screenshot shows the official WFP website page for Haiti relief. The header includes navigation links like 'Chi siamo', 'Pubblicazioni', 'Foto', 'Video', 'Contatti', and a language selector set to 'Italiano'. There is a search bar and a 'DONAZIONI' button. The main navigation bar features the WFP logo, the text 'Programma Alimentare Mondiale' and 'Combatte la fame nel mondo', and buttons for 'LA FAME', 'COSA FACCIAMO', 'COME AIUTARE', and 'NOTIZIE'. The main content area is titled 'Aiutiamo Haiti' and contains a map of Haiti with the text 'Stiamo aiutando Haiti. Fallo anche tu. Dona ora. Aiuta Haiti.' Below this, there is a paragraph describing the earthquake in Haiti and the need for food. A call to action says 'Aiutaci a raggiungere chi ha bisogno. Dona ora.' and lists donation methods: online, bank transfer, and postal transfers. On the right side, there are two blue buttons: 'DONAZIONI - GESTISCI LA TUA PAGINA DELLE DONAZIONI' and 'DICHIARAZIONE SULLA PRIVACY'. Below the first button is a link 'Accedi alla tua pagina delle donazioni' and a paragraph about managing donations. Below the second button is the text 'La tua privacy è importante per noi' and 'Il WFP non cederà i tuoi dati personali a terzi.'

Nel chiedere di voler cortesemente attirare l'attenzione degli utenti internet sulla presente email e invitandoli ad inviare l'eventuale offerta mediante i siti istituzionali, si richiamano alcuni

CONSIGLI

Per proteggersi dal phishing è utile adottare queste precauzioni :

- 1) Non rispondere mai a richieste di informazioni personali giunte sulla casella di posta elettronica. Nessuna Autorità si avvale mai

di strumenti elettronici non certificati per contattare gli interessati al fine di notificargli eventuali provvedimenti o qualsiasi altra notizia che li possa riguardare.

- 2) In caso di ricezione di messaggi che richiedono denaro e/o dati personali, accertare di persona anche tramite telefono, la veridicità del messaggio ricevuto; in ogni caso **evitare sempre di cliccare sul link proposto dall'email**, uscire dalla email e raggiungere il sito voluto digitando il rispettivo U.R.L. (nome del sito)
- 3) Verificare che il sito web del mittente utilizzi la crittografia. Per accertarlo è sufficiente verificare se sulla barra di stato, ai piedi dello schermo, sulla destra, è presente l'icona del lucchetto chiuso, che sta ad indicare che quel sito utilizza una connessione protetta. Cliccandoci sopra due volte è possibile visualizzare il certificato di protezione del sito; il nome che segue **Rilasciato a** dovrebbe corrispondere al sito d'interesse, se è diverso potrebbe essere contraffatto.
- 4) Segnalare immediatamente alla Polizia Postale e delle Comunicazioni eventuali tentativi di carpire i propri dati personali per fini illeciti non andati a buon fine attraverso l'inoltro all'indirizzo poltel.pe@poliziadistato.it del messaggio ricevuto. La tempestività della segnalazione o della denuncia presso l'Autorità competente può permettere che altri soggetti possano incorrere in simili truffe.
- 5) Giova ricordare che i messaggi di phishing offrono un link attivo per sole 24-48 ore, trascorse le quali diventa impossibile rintracciare il sito truffa.

Pescara, 26 gennaio 2010