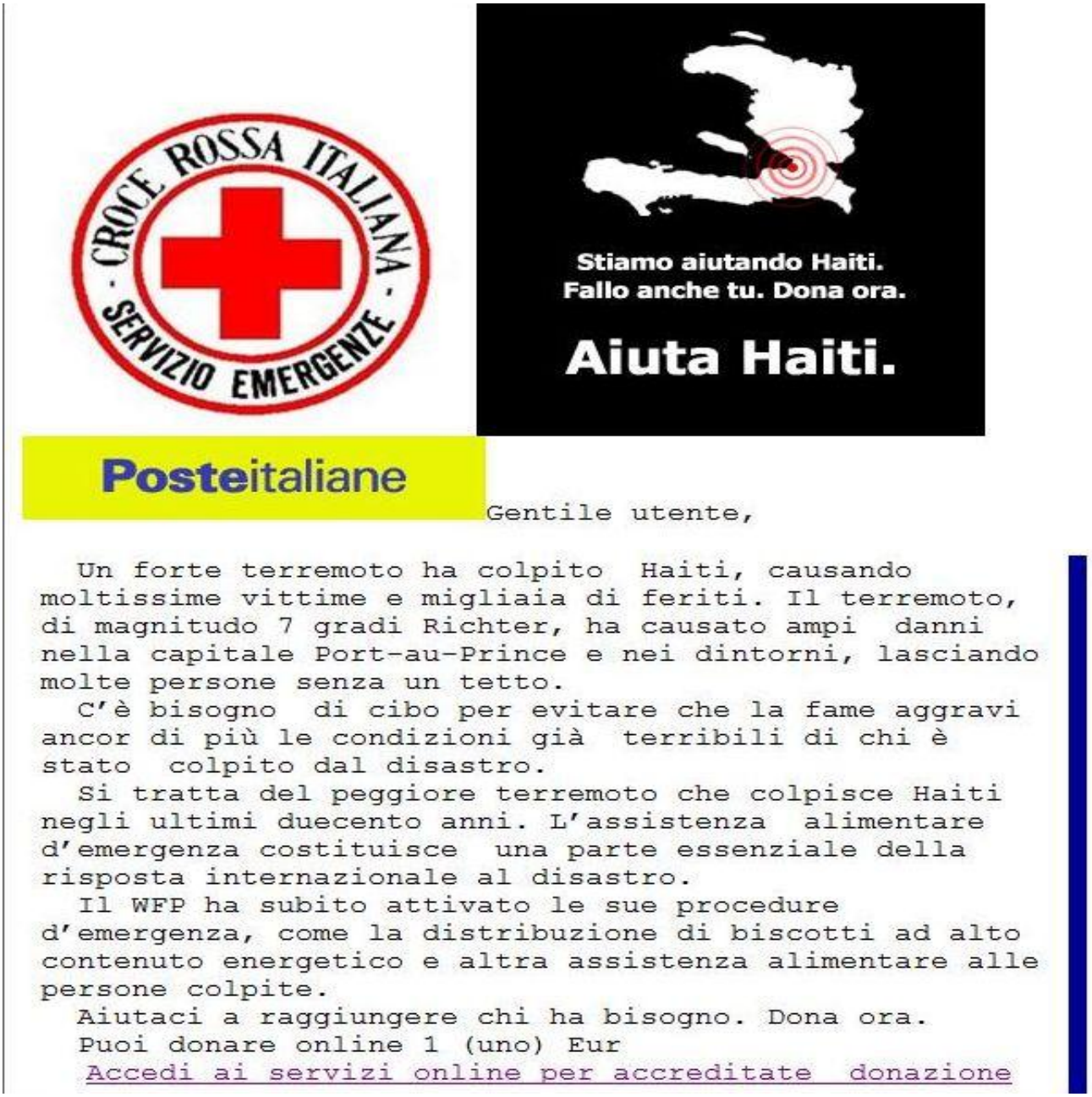
ALLARME PHISHING "PRO TERREMOTO HAITI"

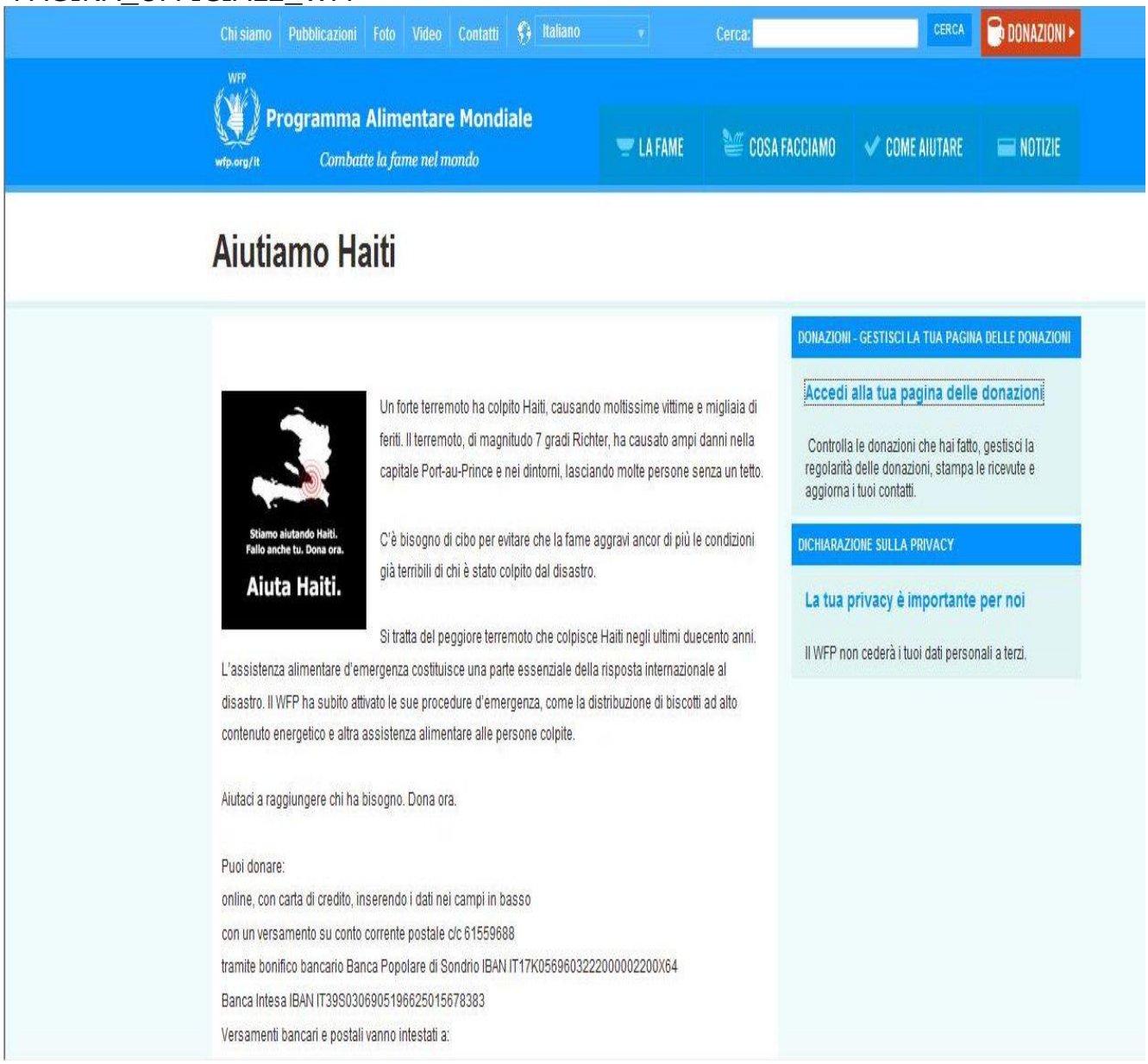
In questi giorni sono stati posti in circolazione diversi messaggi di phishing che, invitando ad effettuare una donazione "pro terremotati Haiti", tentano di carpire i dati personali per l'accesso ai conti correnti on line degli utenti.



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



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