Bollettino di sicurezza del 19 Giugno 2020
Galleria di esempi di tentativi di phishing in atto

Gentilissimi utenti,
pubblichiamo questo bollettino di sicurezza per darvi una galleria di esempi reali di email malevole che in questi mesi hanno raggiunto le nostre caselle di posta elettronica dell'Ateneo. Ogni esempio è seguito da una analisi dettagliata come indicato nella guida disponibile al link:

https://work.unimi.it/filepub/sicurezza_ict/20191210_GuidaPraticaAnalisiMail_v2.pdf

Ricordiamo che l'unico servizio abilitato al cambio della password della posta elettronica e degli altri servizi di ateneo è:

https://auth.unimi.it/password

e che per qualunque problema relativo alla posta di Ateneo (ad esempio spazio esaurito, cancellazione di email e simili) occorre aprire un ticket presso l'Ufficio Servizi di Rete all'indirizzo:

https://auth.unimi.it/servicedesktlc

Vi chiediamo di prestare particolarmente attenzione nel caso dobbiate cambiare la password o abbiate necessità di assistenza per la posta ad utilizzare esclusivamente i link indicati.

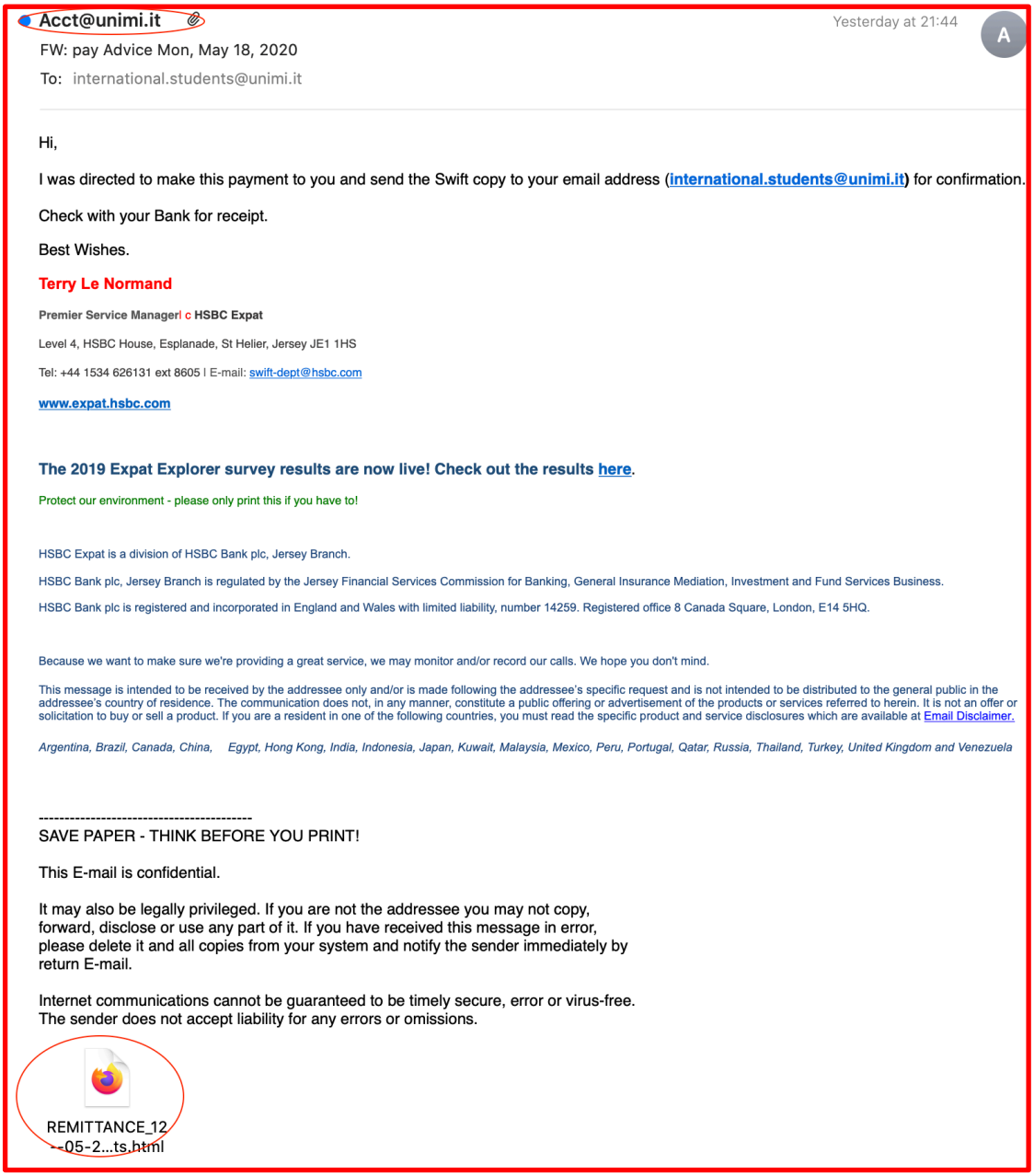
Grazie per la collaborazione e buon proseguimento di lettura.

I più cordiali saluti.

Settore Cybersecurity, Protezione Dati e Conformita' - Direzione ICT
Universita' degli Studi di Milano
Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

Email che chiede di verificare un bonifico

Il primo caso che vogliamo mostrare è relativo ad una mail indirizzata ad un nostro ufficio di assistenza studenti il cui oggetto è la richiesta di verifica di un bonifico che dovrebbe essere stato eseguito dal mittente. La pericolosità di questo tipo di mail risiede nel fatto che non chiede denaro, attività che potrebbe insospettire il destinatario, ma anzi prospetta un bonifico in entrata. Lo scopo è sviare l'attenzione del destinatario sull'allegato che consiste in un finto pdf protetto da password.



Acct@unimi.it
Yesterday at 21:44
FW: pay Advice Mon, May 18, 2020
To: international.students@unimi.it

Hi,

I was directed to make this payment to you and send the Swift copy to your email address (international.students@unimi.it) for confirmation.

Check with your Bank for receipt.

Best Wishes.

Terry Le Normand

Premier Service Manager | c HSBC Expat

Level 4, HSBC House, Esplanade, St Helier, Jersey JE1 1HS

Tel: +44 1534 626131 ext 8605 | E-mail: swift-dept@hsbc.com

www.expat.hsbc.com

The 2019 Expat Explorer survey results are now live! Check out the results here.

Protect our environment - please only print this if you have to!

HSBC Expat is a division of HSBC Bank plc, Jersey Branch.

HSBC Bank plc, Jersey Branch is regulated by the Jersey Financial Services Commission for Banking, General Insurance Mediation, Investment and Fund Services Business.

HSBC Bank plc is registered and incorporated in England and Wales with limited liability, number 14259. Registered office 8 Canada Square, London, E14 5HQ.

Because we want to make sure we're providing a great service, we may monitor and/or record our calls. We hope you don't mind.

This message is intended to be received by the addressee only and/or is made following the addressee's specific request and is not intended to be distributed to the general public in the addressee's country of residence. The communication does not, in any manner, constitute a public offering or advertisement of the products or services referred to herein. It is not an offer or solicitation to buy or sell a product. If you are a resident in one of the following countries, you must read the specific product and service disclosures which are available at Email Disclaimer.

Argentina, Brazil, Canada, China, Egypt, Hong Kong, India, Indonesia, Japan, Kuwait, Malaysia, Mexico, Peru, Portugal, Qatar, Russia, Thailand, Turkey, United Kingdom and Venezuela

---
SAVE PAPER - THINK BEFORE YOU PRINT!

This E-mail is confidential.

It may also be legally privileged. If you are not the addressee you may not copy, forward, disclose or use any part of it. If you have received this message in error, please delete it and all copies from your system and notify the sender immediately by return E-mail.

Internet communications cannot be guaranteed to be timely secure, error or virus-free. The sender does not accept liability for any errors or omissions.

REMITTANCE_12--05-2...ts.html

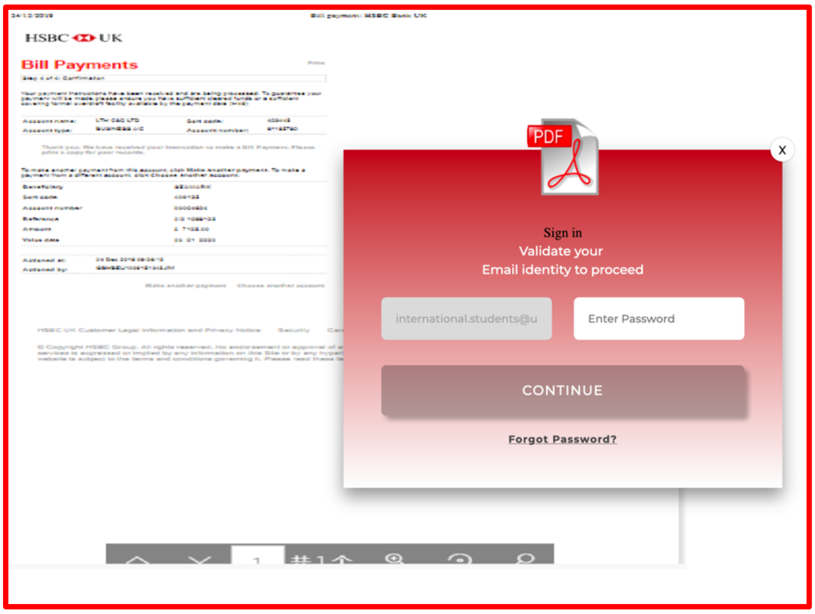
Da notare il From falsificato, Acct@unimi.it, come si vedrà meglio nell'header riportato sotto e l'allegato in formato HTML che può nascondere link e codice malevolo.

Di seguito potete vede l'header nascosto della mail:

```
Received: from unimix2.unimi.it ([[redacted]])
 [redacted]
 for international.students@unimi.it; Mon, 18 May 2020 21:44:31 +0200 (CEST)
Original-recipient: rfc822;international.students@unimi.it
Return-path: <wyss@futurnet.es>
Received-SPF: Pass (sender SPF authorized) identity=mailfrom;
 client-ip=62.97.84.56; helo=mail.futurvia.es; envelope-from=wyss@futurnet.es;
 receiver=international.students@unimi.it
Authentication-results: unimix2.unimi.it; dkim=permerror (bad message/signature
 format)
Received: from mail.futurvia.es (sulley.futurvia.es [62.97.84.56])
    (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
    (No client certificate requested) by unimix2.unimi.it (Postfix)
 with ESMTPS id [redacted] for <international.students@unimi.it>; Mon,
 18 May 2020 21:44:20 +0200 (CEST)
Received: from mail.futurnet.es (unknown [46.183.222.17])
    (Authenticated sender: wyss@futurnet.es)  by mail.futurvia.es (Postfix)
 with ESMTPSA id [redacted] for <international.students@unimi.it>; Mon,
 18 May 2020 21:44:18 +0200 (CEST)
From: Acct@unimi.it
To: international.students@unimi.it
Subject: FW: pay Advice Mon, May 18, 2020
Date: Mon, 18 May 2020 22:44:50 +0300
Message-id: <2[redacted]
MIME-version: 1.0
```

Da notare la discrepanza tra campo From, Acct @ unimi.it, usualmente mostrato dai client di posta ed in questo caso falsificato, e il campo envelope-from, wyss @ futurenet.es, che indica il reale dominio di partenza della mail.

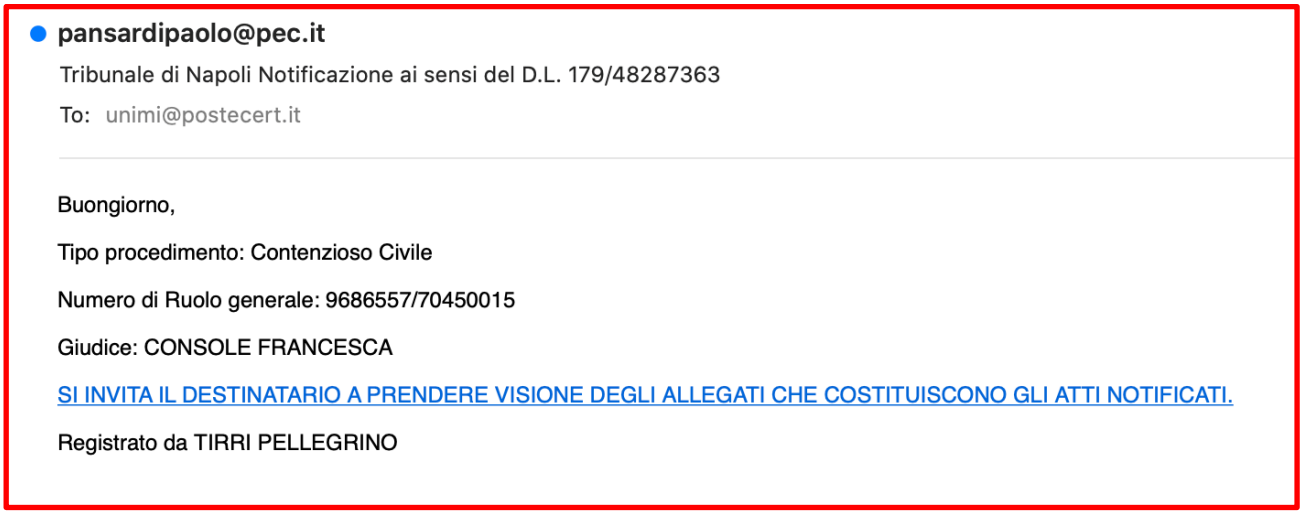
Se si apre l'allegato, operazione da non eseguire in presenza degli elementi sopra riportati in quanto chiaramente malevolo, si visualizza una pagina HTML in locale che mima un documento PDF protetto da password:



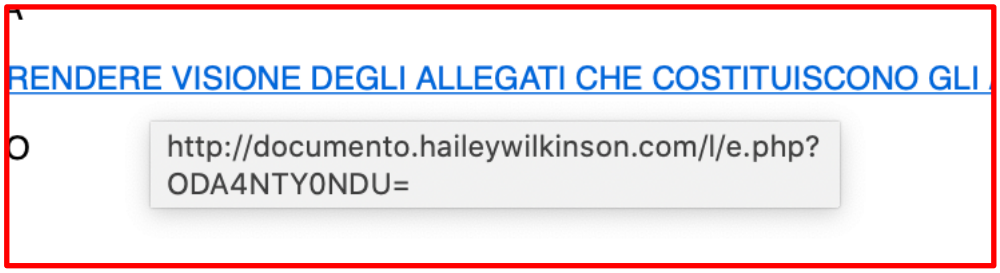
L'inserimento delle credenziali all'interno del form provoca l'invio delle stesse ad un sito estero.

Email che segnala un documento in attesa

Il secondo caso che riportiamo è una mail che segnala un documento connesso ad una causa legale in attesa di essere visionato. Il documento solitamente consiste nel primo stadio di un malware teso alla compromissione del PC dell'obbiettivo. La mail può presentarsi come segue:



Posizionandosi sopra il link con il mouse è possibile sui maggiori client di posta visionare link in anteprima:



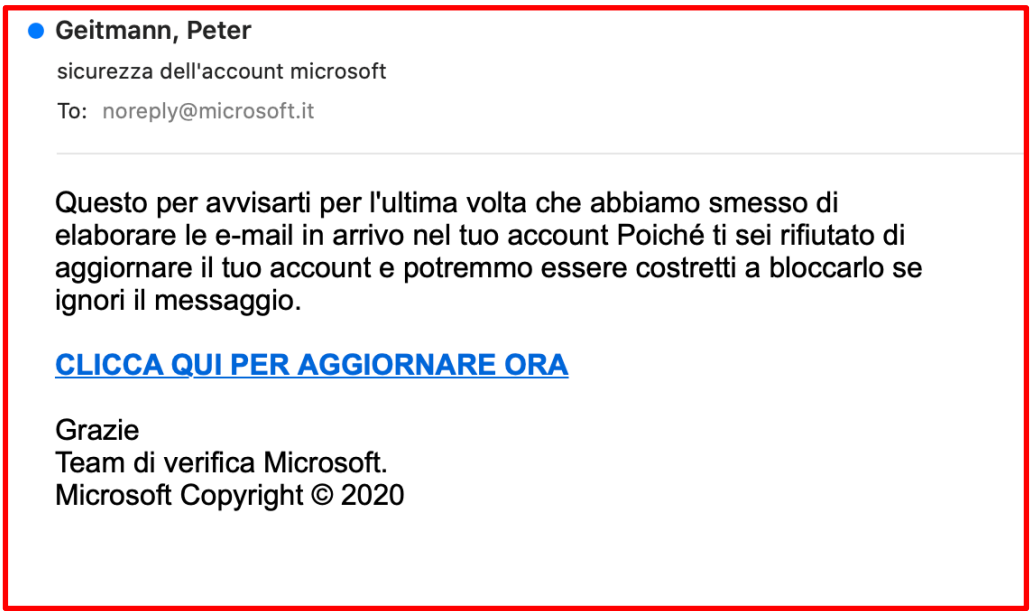
Qualora l'utente segua il link, il browser viene portato attraverso vari salti successivi su una share Dropbox, Google Drive o altri servizi simili allo scopo di aumentare la reputazione del documento messo in share. Generalmente alla fine dei salti è presente un documento Microsoft Office contenente codice macro malevolo che se eseguito scarica il vero e proprio virus da un ulteriore sito.
In questo tipo di attacchi, ciò che dovrebbe insospettire sono i seguenti fatti:

- La mail non è sollecitata e di tono allarmistico;
- Il link indicato è di tipo HTTP e rimanda ad un sito sostanzialmente anonimo, non istituzionale;
- Spesso il documento finale è di tipo Office che richiede l'esecuzione di codice.

Buona norma per difendersi meglio da questo genere di attacchi è verificare che non sia abilitata l'esecuzione automatica delle macro nei documenti Office.

Email che segnala un problema con la posta elettronica

Quasi giornalmente sulle nostre caselle di posta arrivano tentativi di phishing tesi a sottrarre le credenziali di accesso ai servizi di Ateneo. Di seguito rimportiamo alcuni esempi:



Geitmann, Peter

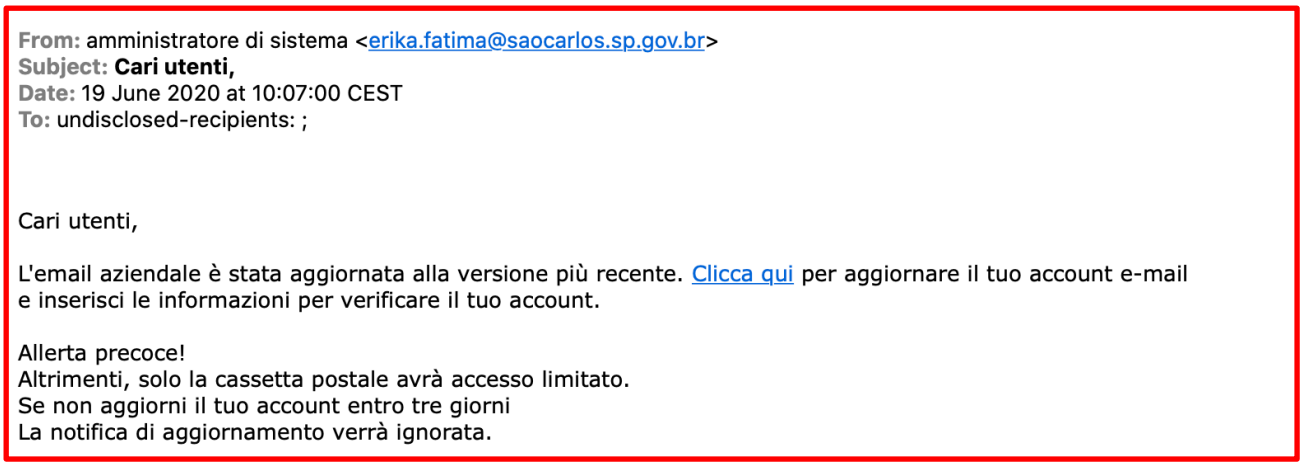
sicurezza dell'account microsoft

To: noreply@microsoft.it

Questo per avvisarti per l'ultima volta che abbiamo smesso di elaborare le e-mail in arrivo nel tuo account Poiché ti sei rifiutato di aggiornare il tuo account e potremmo essere costretti a bloccarlo se ignori il messaggio.

CLICCA QUI PER AGGIORNARE ORA

Grazie
Team di verifica Microsoft.
Microsoft Copyright © 2020



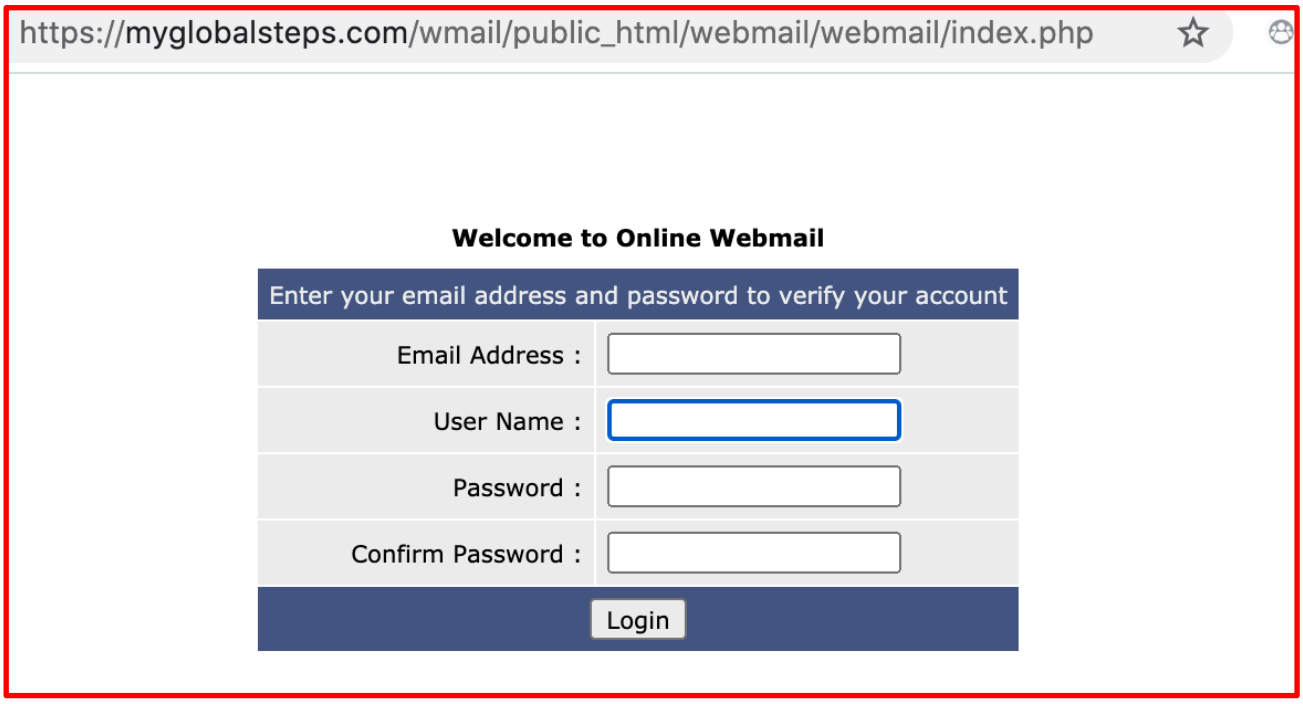
From: amministratore di sistema <erika.fatima@saocarlos.sp.gov.br>
Subject: **Cari utenti,**
Date: 19 June 2020 at 10:07:00 CEST
To: undisclosed-recipients: ;

Cari utenti,

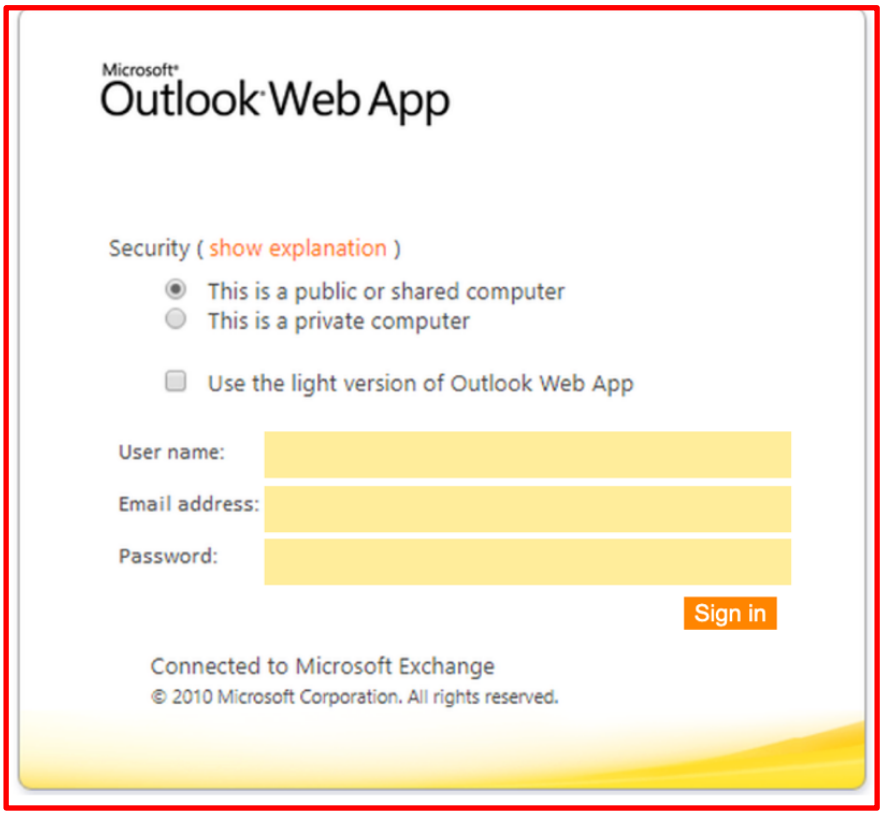
L'email aziendale è stata aggiornata alla versione più recente. Clicca qui per aggiornare il tuo account e-mail e inserisci le informazioni per verificare il tuo account.

Allerta precoce!
Altrimenti, solo la cassetta postale avrà accesso limitato.
Se non aggiorni il tuo account entro tre giorni
La notifica di aggiornamento verrà ignorata.

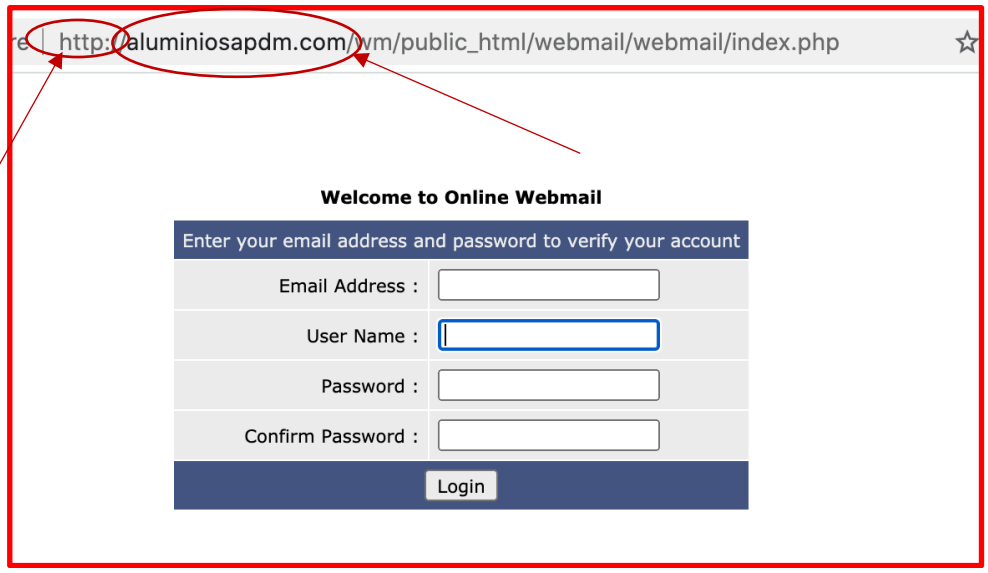
Come nel caso precedente, se l'utente segue il link viene condotto su un sito malevolo in cui viene chiesto di inserire le proprie credenziali. Di seguito è riportato un esempio più semplice:



A volte il sito di phishing è particolarmente curato:



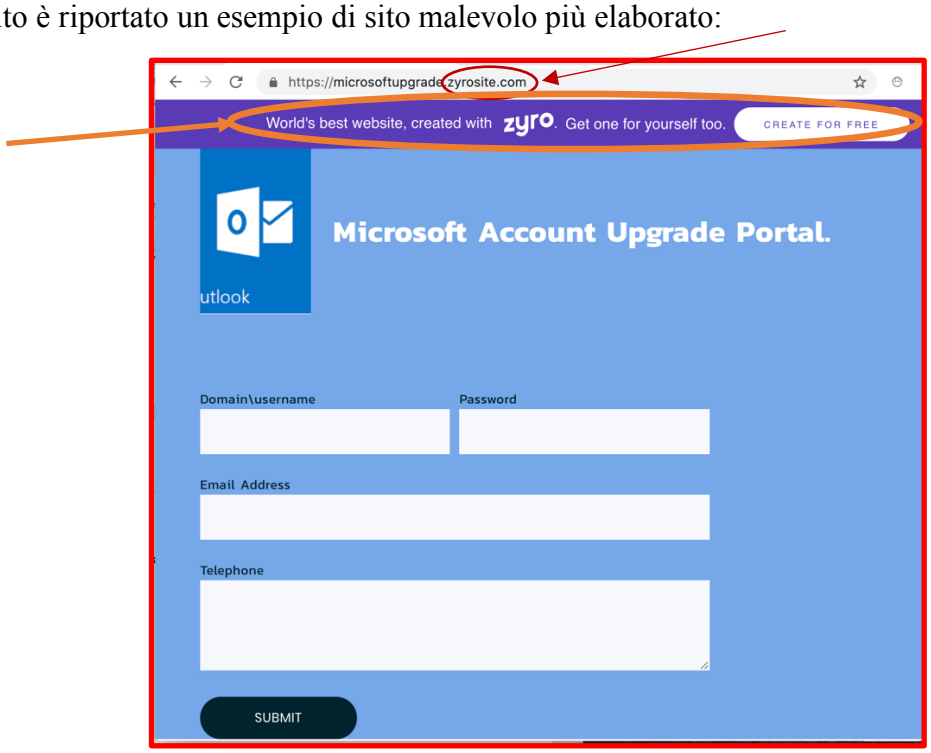
In tutti i casi prima di inserire le credenziali occorre prestare particolare attenzione alla barra dell'indirizzo sul browser. Qui di seguito è riportato un esempio di sito di phishing:



Osservando con attenzione la barra dell'indirizzo si può notare che

- il protocollo usato è HTTP non adatto alla trasmissione di credenziali
- il dominio che ospita il sito, aluminiosapdm[.]com, non è un dominio istituzionale.

Di seguito è riportato un esempio di sito malevolo più elaborato:



In questo caso, pur usando HTTPS, il sito ospitante, zyrosite[.]com, non è un sito istituzionale dell'Ateneo né di Microsoft. In aggiunta, si può notare che il sito ospitante è un sito per la creazione di pagine web gratuita e generalmente senza particolari meccanismi di verifica dell'identità del web designer.