Phishing and malware - how to recognize it

Come riconoscerlo

Google page with infos about phishing

Esempi
1- fake univr email
Example May 2018

Gentile utente di univr.it,

Stiamo aggiornando i nostri account webmail di univr.it al fine di aumentare il l'efficienza delle funzionalità del nostro account e la modifica della visualizzazione della home page.

Abbiamo notato che il tuo account non è stato aggiornato alla nostra nuova web mail sistema, devi confermare lo stato del tuo account in modo che possiamo

procedi con l'aggiornamento del tuo account e aumenta il tuo spazio di
archiviazione

spazio, qualsiasi utente che non ha confermato il proprio account sarà permanentemente perdere il suo account per consentirci di creare più spazio per il nuovo utenti.

Fai clic sulla scheda di risposta e fornisci i tuoi dettagli di seguito:

Nome utente:

Parola d'ordine:

Data:

Telefono:

Indirizzo email alternativo:

Speriamo che apprezzerai il nostro nuovo sistema di upgrade e ti promettiamo di darti la migliore navigazione internet.

Grazie per aver utilizzato la webmail di univr.it

dipartimento tecnico di univr.it.

Example August 2018

[Institutional Communication] Verifica il tuo account e-mail univr.it ora

Gentile utente dell'account e-mail di univr.it,

La dimensione della tua casella di posta ha raggiunto il limite di quota stimato e alcuni dei tuoi messaggi in arrivo sono in sospeso sul nostro erver

a causa di questo problema, devi aggiornare il tuo account per evitare di superare il limite di quota e aspettare qualche ora mentre verifichiamo e rettifichiamo e anche per consentire l'esecuzione di operazioni di aggiornamento e manutenzione straordinaria.

Si prega di compilare di seguito:

Indirizzo email:

Nome utente:

Parola d'ordine:

Il mancato aggiornamento potrebbe comportare la chiusura del tuo account di posta elettronica.

Grazie

The Director of Information Systems and Technologies Management

Dr. Giovanni Bianco

What you should do

Do NOT send your credentials and cancel the email.

2- fake RePec site (July 2018)

quando si cercano pubblicazioni con google nei risultati si trovano a volte dei link su siti che sembrano essere collegati con la piattaforma delle pubblicazioni economiche RePec.

In realtà bloccano il browser, dicono che c'è un virus sul pc e chiedono di inserire le proprie credenziali.

Esempio di sito malevole: ideas. repec. yadoedu. ru :

Do NOT insert your credentials in any case and close the browser with the task manager.

3- email from fake lawyer's office (July 2018)

Title: Relazione di notifica decreto
No.3719755742 Del 14/06/18

Io scrivente Avvocato Luigi
Marinelli con studio a Arezzo situato in LARGO MATTIOLI
RAFFAELE
, 662 P.IVA:83548326547 nella mia qualità di difensore e domiciliatario del Sig. Antonio
Rossi, res. a Arezzo indirizzo LARGO MATTIOLI RAFFAELE
, 175

COMUNICO

Ad ogni risultato di legge l’atto N. 3719755742 in originale informatico

Che lo po visualizzare al seguente indirizzo web: <Link
to bad site>
(ovvero) in copia digitale conforme all’originale informatico da me predisposto nel giudizio civile dinanzi al Tribunale di Ar
o, mediante invio di email di posta elettronica dalla mia casella, e con ricevuta completa, all’indirizzo
<your email>

Attesto infine che il messaggio , oltre alla presente relata di notifica sottoscritta digitalmente, contiene il seguente Atto che lo po s
re al seguente indirizzo web: Atti anch’essi sottoscritti digitalmente: – copia informatica della decreto.

If you click on the link it downloads a zip file that contains an image and a .vbs that activates a trojan.

4- email asking to pay through Bitcoin (October 2018)

In questi giorni sono stati segnalati vari casi di mail (in lingua
italiana o inglese) in cui si dichiara di essere in possesso di
materiale compromettente e se ne minaccia la diffusione, invitando al
pagamento di una somma in valuta virtuale.

Si tratta di mail fraudolente del tipo "black mirror", di cui si sono occupati anche gli organi di informazione a livello nazionale.

The email tells you some hackers did successfully get access to all of the data on your computer and will send some compromising information about you to all of your contacts. It then asks you to pay through Bitcoin in order not to send this information.

Do NOT pay in any case! Your money will be lost with no possibility to trace it.

To be on the safe side change the password of the account the email was sent to (if it was sent to @univr.it change your GIA credentials).

If you are unsure run an antivirus scan on your pc. If you are still unsure uninstall the antivirus and run the check with an other one.Check if the pc has strange behaviours.In worst case format your pc.

5- fake email from UniVR IT staff (October 2018)

Da: <UniVR user>

Inviato: giovedì 18 ottobre 2018 01:42

Oggetto: MANUTENZIONE DEL CONTO /
AGGIORNAMENTI

Gentili tutti gli utenti di Webmail UNIVR

Al momento, stiamo effettuando la
manutenzione, in modo che tutti gli account di posta
elettronica vengano aggiornati per la verifica. Questa
manutenzione viene eseguita per ridurre il numero di
account e-mail inattivi nel nostro database. Gli account
e-mail non verificati verranno sospesi entro 48 ore.

Si prega di "<LINK CLICCA QUI>" e
seguire le istruzioni.

webmaster

Università di Verona (UNIVR)

Oggetto: Ultimo avviso aggiorna la tua email.

Data: Wed, 7 Nov 2018 12:19:35 +0000

Mittente: E-mail institucional DPCOM do CPP <cpp.dpcom@pm.df.gov.br>

Il limite di archiviazione della tua casella di posta elettronica è stato superato a causa dell'elevato tasso di spam / mail, tutti i messaggi in arrivo sono attualmente rifiutati. Per convalidare nuovamente la tua e-mail, fai clic sul link sottostante e compila il modulo per aumentare il limite della tua quota email.

Clicca qui: <bad link>

Avvertimento. Tutti i proprietari di account di posta elettronica che si rifiutano di aggiornare il proprio account entro 24 ore dalla ricezione di questa email perderanno il loro account in modo permanente.

Grazie per la collaborazione!

Servizio tecnico webmail

Do NOT CLICK ON THE LINK! Usually they try to steal your credentials (so called "phishing").

You can select the email in the list and choose "Posta indesiderata > Phising" in the upper menù of the webmail in this case.

In this way the messages are more likely to be moved in the "Posta indesiderata" directory or will be even blocked directly by Outlook.

Empty your "Spam" folder from time to time.

6- Email with attachment (November 2018)

Buongiorno,

Vedi allegato e di confermare.

<Name of a person you know>

Address, xx - yyyy city

t +xx xx xxxxxx

f +xx xx xxxxxx

m +xx xx xxxxxx

Attached is a Word file with a Macro

Do not open the Word file and do NOT accept to execute the Macro in any case.

7- Fake e-mail from UniVR staff (december 2019)

Da: E-Mail Account Notice @048230032780428630429 [mailto:mharrison@artconsultingservices.net]

Inviato: lunedì 9 dicembre 2019 14:11

A: xxx.yyy@univr.it

Oggetto: War-ni-ng You xxx.yyy@univr.it

Microsoft Outlook Notice

You can no longer sign in your Email xxx.yyy@univr.it

because it was close down today

And you can't send or receive mail anymore

Date: 12/9/2019

Update To Stay Active <bad link>

Thanks,

Microsoft Account Team

Same indications as 5-

Come segnalare phishing

Se si tratta di una email si può segnare come "spam" o "phishing" nella webmail : selezionare il messaggio nell'elenco e la voce di menù "Posta indesiderata > Phishing"

Segnalare a UniVR: inviare il messaggio come allegato zippato ai tecnici di riferimento che inoltrano ai colleghi dell'Helpdesk centrale (con Windows e Firefox ad esempio: selezionare il messaggio, mouse destro, salva come, il file viene salvato in formato .eml, selezionare il file, mouse destro, invia a, cartella compressa)

Segnalare a google: https://safebrowsing.google.com/safebrowsing/report_phish/?hl=it

Segnalare a Yahoo (necessario avere email yahoo): https://safety.yahoo.com/Security/REPORTING-ISSUES.html

Segnalare a Bing:

Segnalare a Microsoft: Aprire Internet Explorer, digitare l'indirizzo
del sito, mouse destro, Strumenti, Filtro Windows Defender Smart Screen,
Segnala sito web come non sicuro.

Chiudere la finestra con l'indirizzo malevole prima di compilare.

Segnalare al servizio anti-frode dell'associazione consumatori tedeschi (Verbraucherzentrale):

inoltrare la email di phishing a phishing@verbraucherzentrale.nrw (non rispondono).Vedi info sul servizio (in tedesco)

Vedi anche indicazioni qui: https://www.aranzulla.it/come-segnalare-un-sito-truffa-1062237.html

Elenchi di siti fraudolenti

Siti segnalati da banca francese