IMPARA A DISTINGUERE IL VERO DAL FALSO

OBIETTIVI

Capire cos'è il pishing

Riconoscere i tentativi di frode

Affrontare Sconosciuti in rete

IL PISHING

PISHING

IL PHISHING

Truffa per rubare password, credenziali o informazioni rilevanti

IL PHISHING

Link per verificare account personali al fine di rafforzare la sicurezza o in cambio di benefici o servizi gratuiti

IL PHISHING

Ottenere l'accesso da remoto

IL PHISHING

Mail

Catene

Link

IL PHISHING

Per questo motivo è importantissimo prestare sempre la massima attenzione al controllo dei propri account sul web e attivare nella casella di posta i filtri antispam

ATTENZIONE!

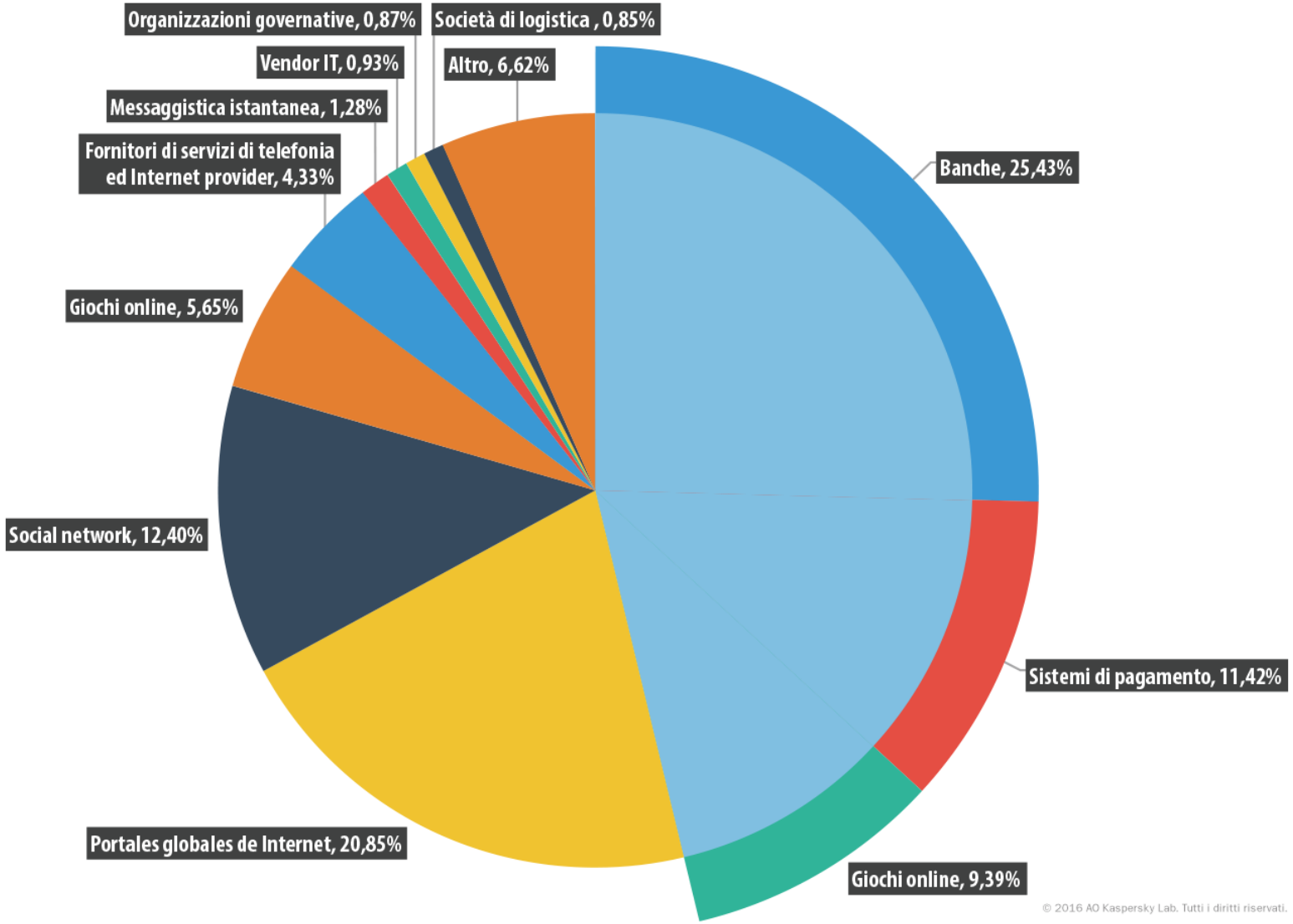
Bisogna sempre verificare con attenzione un messaggio che offre in modalità completamente gratuita qualcosa che ha un valore economico oggettivo

ATTENZIONE!

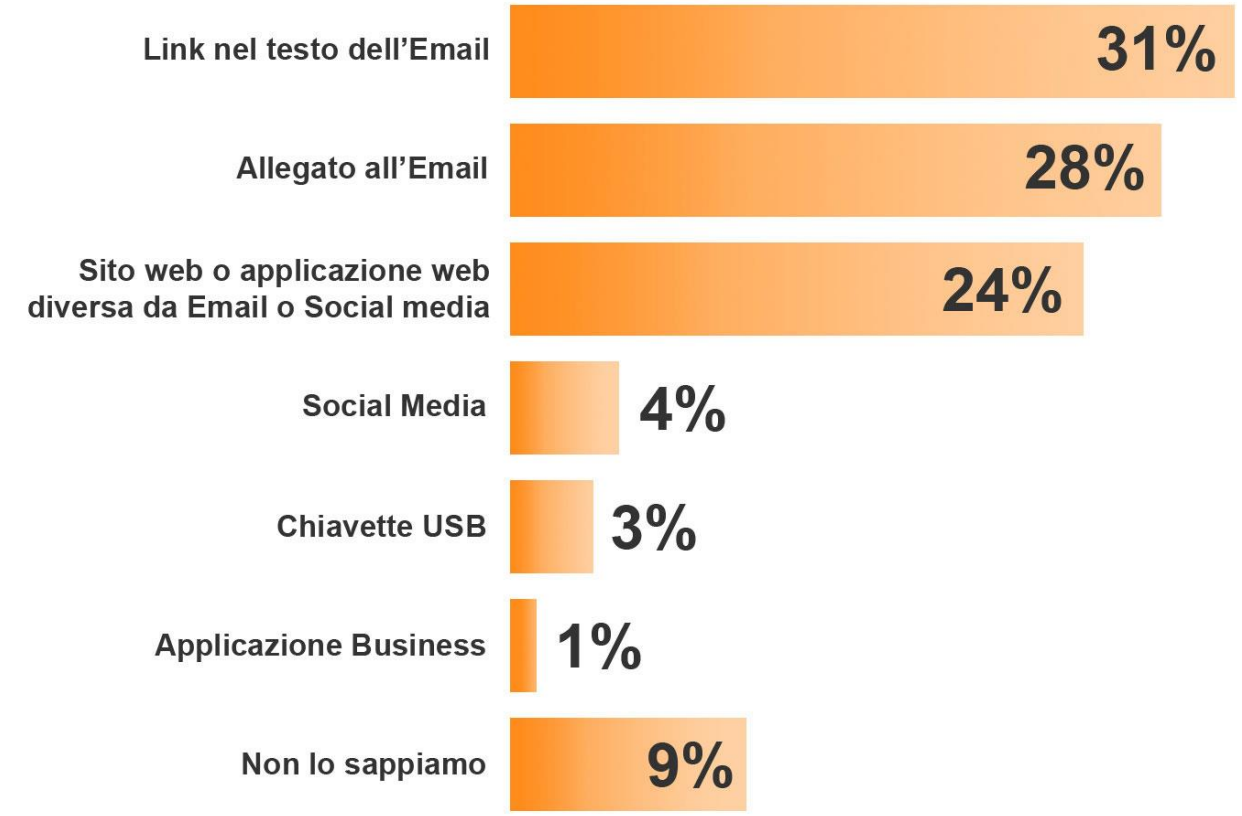
E i social?

IL PHISHING

Banche, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso email, sms, social media o chat


Organizzazioni governative, 0,87%
Società di logistica , 0,85%
Vendor IT, 0,93%
Altro, 6,62%
Messaggistica istantanea, 1,28%
Fornitori di servizi di telefonia ed Internet provider, 4,33%
Banche, 25,43%
Giochi online, 5,65%
Social network, 12,40%
Sistemi di pagamento, 11,42%
Portales globales de Internet, 20,85%
Giochi online, 9,39%
© 2016 AO Kaspersky Lab. Tutti i diritti riservati.

Da dove entra in azienda il malware



Fonte: Osterman Reasearch, Inc.

RICONOSCERE I TENTATIVI DI FRODE

NELL'EMAIL O IN CHAT TI VIENE OFFERTO QUALCOSA GRATUITAMENTE?

TI VENGONO RICHIESTE INFORMAZIONI PERSONALI?

SI TRATTA DI UNA CATENA O DI QUALCOSA CHE LE ASSOMIGLIA?

CONTIENE PORZIONI DI TESTO SCRITTE IN PICCOLO?

CASO 1

Uno di voi riceve questo messaggio sul cellulare in merito ad una notissima marca di abbigliamento "Buono di 150€. Ricevi un coupon di Adidas del valore di 150€ clicca su adidas.coupongratis.com. Io l'ho appena preso, sbrigati non perdere tempo! :D" Lo gira a tutta la classe e anche a te, pensando di fare una cosa gradita

COSA LE CONSIGLIERESTE DI FARE?

Ignorare il messaggio e non cliccare
Cliccare per capire di cosa si tratta
Inviarlo a quante più amiche possibili
Diffidare in futuro di questo tipo di messaggi e cancellarlo senza cliccare sul link
Informare tutta la classe delle truffe che si nascondono dietro questo tipo di messaggi

PRESTARE ATTENZIONE

Indirizzo email associato al messaggio/commento

PRESTARE ATTENZIONE

Il link contiene un dominio molto simile ma non completamente uguale a quello reale (ad esempio www.gooogle.it al posto di www.google.it)

PRESTARE ATTENZIONE

Il messaggio contenuto è in inglese o in un'altra lingua diversa dall'italiano

PRESTARE ATTENZIONE

L'allegato contiene una doppia estensione: nome.pdf.exe, o un'estensione strana come .pif e cliccandovi due volte si esegue invece un file malevolo

ESEMPIO

Immaginiamo una ipotetica piattaforma di musica in streaming, il cui dominio Internet (inesistente e ideato solo ai fini del game) è teenmusic.it.

Tutti gli indirizzi web (URL) e gli indirizzi email che troveremo nelle email provenienti da questa piattaforma dovranno essere quindi del tipo: teenmusic.it/login, xyz.teenmusic.it, xyz@teenmusic.it

ESEMPIO TENTATIVI DI FRODE

1db3w0assistenza@teen-music.com

ESEMPI TENTATIVI FRODE

http://online.da.teenmusic.da-it.update.com

ESEMPI TENTATIVI FRODE

https://titolari.teenmusic.it/server.pt

ESEMPI TENTATIVI FRODE

http://kolems.cz/teenmusic.it/st.php

ESEMPI TENTATIVI FRODE

http://login.teenmusic.access.it

ESEMPI TENTATIVI FRODE

assistenza@teenmusic.ru

ESEMPI TENTATIVI FRODE

http://80.574.215.39.teenmusic-italia.it

ESEMPI TENTATIVI FRODE

noreply@teenmusic.it

ESEMPI TENTATIVI FRODE

www.teenmusic.com.personal.login.it

RIESCI A DISTINGUERE QUELLI VERI DA QUELLI FALSI?

1db3w0assistenza@teen-music.com

http://online.da.teenmusic.da-it.upadate.com

https://titolari.teenmusic.it/portal/server.pt

http://kolemsveta.cz/www.teenmusic.it/index.php

http://login.teenmusic.access.it

assistenza@teenmusic.ru

http://80.574.215.39.teenmusic-italia.it

noreply@teenmusic.it

www.teenmusic.com.personal.login

CASO 1

Simona è in ufficio da suo padre e sta usando il suo pc. Controlla la posta e riceve un'email apparentemente inviata dalla sua piattaforma di streaming musicale (legale) preferita, che le promette due mesi di abbonamento gratuito, ma le chiede di scaricare un file allegato da compilare e inoltrare al mittente con i suoi dati.

CASO 1

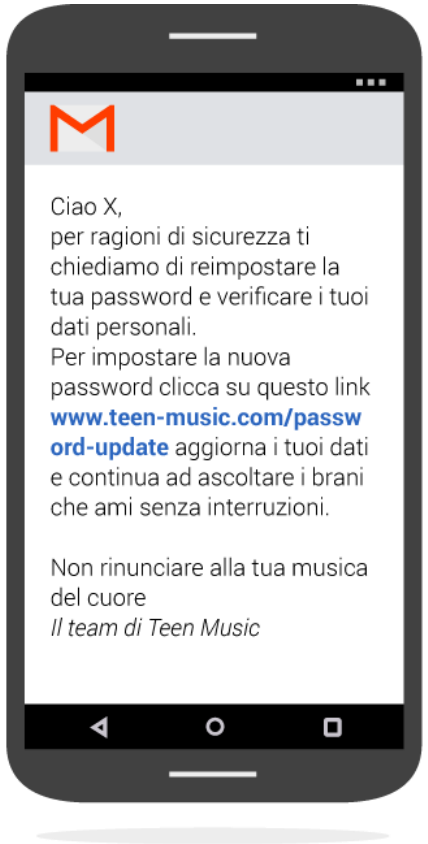
Simona scarica l'allegato e improvvisamente il computer comincia a non rispondere più ai suoi comandi e le si apre una finestra che richiede l'inserimento di una password per sbloccarlo e poter continuare a usare il pc e accedere ai dati e ai file. La password si può ottenere effettuando il pagamento di 500 euro. Simona è terrorizzata, è il pc che suo padre usa per lavorare e su cui ha tantissimo materiale riservato

COSA AVREBBE POTUTO FARE SIMONA?

Controllare l'indirizzo email del mittente
Controllare se l’allegato ha un'estensione immediatamente eseguibile (es. .exe, .bat o ancora .msi)
Contattare la polizia postale
Spegnere il PC nella speranza che si resetti
Staccare la corrente elettrica e non accendere il PC per 7 giorni consecutivi
Scaricare un Antivirus

CASO 2

Lorenzo è registrato sulla popolare piattaforma di musica in streaming, www.teenmusic.it. Il rinnovo è automatico e per questo utilizza una carta prepagata ricaricabile che suo padre ha attivato per lui e che ha registrato sul sito. Lorenzo riceve un'email inviata dal centro clienti della piattaforma in cui gli viene richiesto di aggiornare i dati personali (vedi immagine)



CASO 2

Il mittente è noreply@teen-music.it . Clicca su un link nel corpo della mail, ma si accorge che non finisce sulla solita pagina della piattaforma di musica, ma su una pagina che un po' le assomiglia e comunque ha il logo e i colori di quella di Teen Music. Gli viene chiesto di aggiornare i suoi dati e di reimpostare la password per motivi di sicurezza, chiedendogli però di inserire la password corrente unitamente al Codice Utente. La cosa lo insospettisce e si ferma.

HA FATTO BENE?

SE CADETE VITTIMA DI PISHING

Non disperate, può capitare a tutti

Parlarne subito con i genitori o con un adulto di cui ci si fida

Cambiare le password degli account dove ci sono dati sensibili

Avvisare i contatti

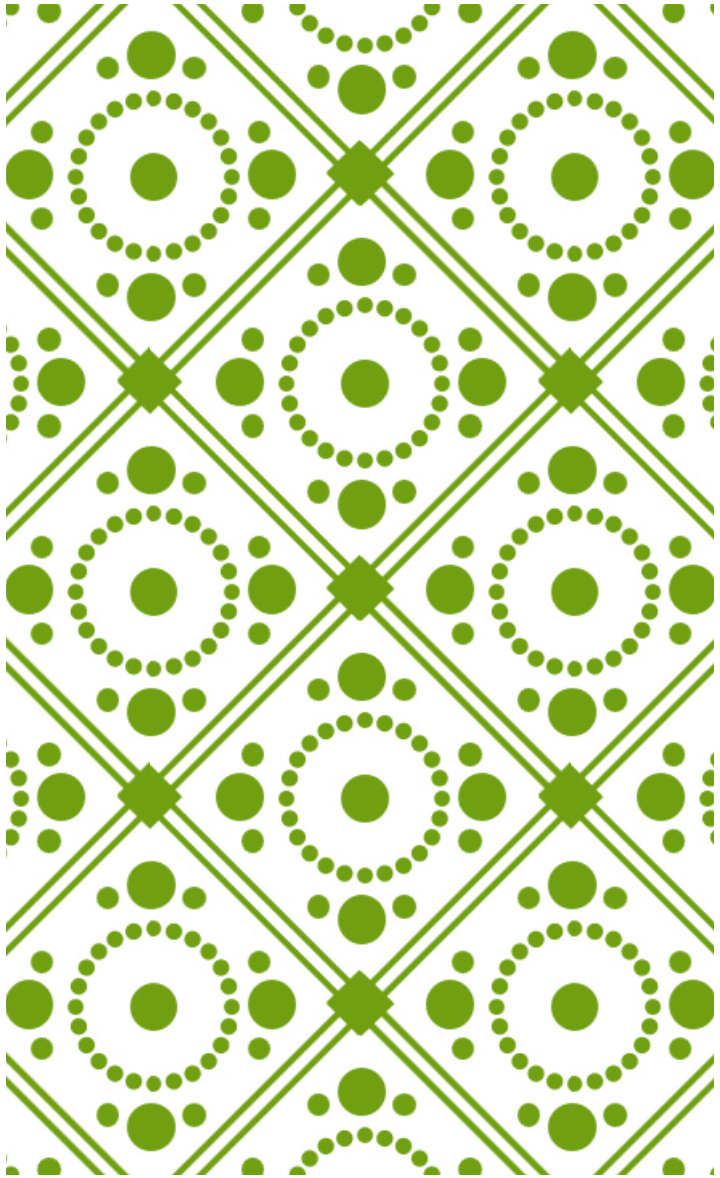
In caso di dubbio, chiedere supporto al Telefono Azzurro

SCONOSCIUTI IN RETE

SCONOSCIUTI IN RETE

A volte le persone fingono di essere qualcun altro online, in alcuni casi per fare degli scherzi, in altri allo scopo di rubare informazioni personali

Fortunatamente, ci sono degli elementi a cui prestare attenzione per verificare l'identità delle persone che ci contattano e identificare potenziali truffatori



L'IMMAGINE DEL PROFILO È REALE E SE REALE È SFOCATA?

SUL PROFILO CI SONO INFORMAZIONI PERSONALI DETTAGLIATE?

DA QUANTO TEMPO ESISTE QUESTO ACCOUNT?

CASO 1

In chat ti scrive qualcuno che non conosci: "Ti ho visto nei corridoi di scuola oggi. 6 adorabile! Qual è il tuo indirizzo? Potrei venire da te x fare 2 chiacchiere."

COSA È PIÙ OPPORTUNO FARE?

Ignorare il messaggio

Bloccare questa persona

Avviare comunque la conversazione con un "Chi sei?"

"Vivo al numero 24 di via Roma, chi sei?"

CASO 2

Ricevi un messaggio da parte di qualcuno che non segui. "Ehi! Adoro i tuoi post, sei troppo divertente! Dammi il tuo numero di telefono, così possiamo parlare un po' e conoscerci meglio"

COSA GLI CONSIGLIERESTE DI FARE?

Di ignorare il messaggio

Di bloccare il contatto

Di rispondere "Ciao, ci conosciamo?" o "Dove ci siamo conosciuti?"

Di scrivergli "Grazie! Il mio numero è..."

PRESTARE ATTENZIONE

https://phishingquiz.withgoogle.com/