POSTA ELETTRONICA

RISCHI E CAUTELE

GLI ATTACCHI PIU' COMUNI

Forzatura di password semplici

GLI ATTACCHI PIU' COMUNI

Forzatura di password semplici

	Count	Password		Count	Password
1	9218720	123456	21	370652	666666
2	3103503	123456789	22	354784	123
3	1651385	qwerty	23	347187	monkey
4	1313464	password	24	343864	dragon
5	1273179	111111	25	311371	1qaz2wsx
6	1126222	12345678	26	300279	123qwe
7	1085144	abc123	27	299984	121212
8	969909	1234567	28	298938	myspac
9	952446	password1	29	291132	a123456
10	879924	1234567890	30	276473	qwe123
11	866640	123123	31	270488	1q2w3e4r
12	834468	12345	32	268121	zxcvbnm
13	621078	homelesspa	33	263605	7777777
14	564344	iloveyou	34	255079	123abc
15	527158	1q2w3e4r5t	35	250732	qwerty123
16	470562	qwertyuiop	36	241721	qwerty1
17	468554	1234	37	241495	987654321
18	417878	123456a	38	227701	222222
19	398114	123321	39	226785	555555
20	371627	654321	40	220363	112233

GLI ATTACCHI PIU' COMUNI

Forzatura di password semplici

<nome_utente> <username>

<nome_figli>+<anno> <nome_coniuge>

<città>+<anno> <indirizzo_sede>

<nome_ente> «12345678»

[combinazioni tasti] (es. 1q2w3e4r, qwerty)

[password brevi]

GLI ATTACCHI PIU' COMUNI

Falsa pagina login

Da: "Postmaster" <mail@post.org>
Inviato: Giovedì, xxx 15:36:32
Oggetto: Postmaster

Il tuo account ha superato il limite di quota impostato dall'amministratore e potresti non essere in grado di inviare o ricevere nuove mail fino a quando non riconvalidi il tuo account. Per riconvalidare l'account, fare clic su: riconvalida account

GLI ATTACCHI PIU' COMUNI

Falsi messaggi da vere PEC

La certezza del mittente non equivale alla veridicità del messaggio…

GLI ATTACCHI PIU' COMUNI

Falsi messaggi da vere PEC

- esposto circa la SOGEI
- candidatura Profilo F1
- 272435426
- Re: Ricevuta protocollo
- Ricevuta protocollo
- INAIL Comunica [9633468]
- Fatture Ottobre 2019
- Revisione elettorale
- Nota prot n 114438 del 18092019
- Piano Triennale per l'informatica nella Pubblica Amministrazione 2017-2019 Definizione dei piani di adesione e attivazione a PagoPA
- Atto amministrativo relativo ad una sanzione amministrativa prevista dal Codice della Strada Nr. V/61254/2019

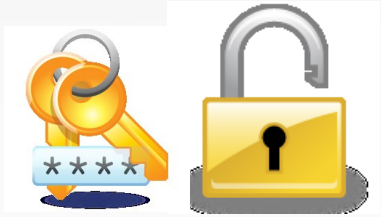
LE POSSIBILI CONSEGUENZE

1) Invio di spam ad altri soggetti

2) Lettura dei messaggi della casella

3) Violazione della postazione

4) Password reuse



CAUTELE

non aprire messaggi di posta contenenti link o .zip;

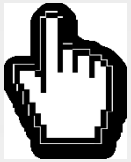
non rispondere ai messaggi che propongono di disattivare l'invio di email successive, sono uno strumento di verifica di esistenza dell'email destinataria;

non abbassare la guardia sui messaggi di utenti conosciuti, potrebbero loro aver contratto un malware;

non aprire comunicazioni contenenti fatture, sanzioni o cartelle esattoriali, avvisi di denuncia…;

i messaggi che cercano di attirare l'attenzione mirano a non far ragionare gli utenti: attenzione alle parole urgente, offerta importante, verifichi subito,…;

CAUTELE



verificare i link prima di aprirli, passandoci sopra con il mouse per vedere dove puntano veramente;

attenzione allo scrivere email in cc a molti indirizzi in contemporanea, si mette in conoscenza ognuno dei destinatari dell'indirizzo degli altri;

non inoltrare dati personali ad indirizzi di email personali (escono dal perimetro del Titolare) e non inviare dati «particolari»;

attenzione alla funzione di autocompletamento degli indirizzi dei destinatari;

non aprire comunicazioni di consegna pacchi da parte di corrieri, è una frode diffusa in certi periodi dell'anno;

Spam e virus

Se ricevi un'e-mail in cui si riporta che DHL sta cercando di consegnare un pacco e ti invita ad aprire un allegato per poter effettuare la consegna, sappi che questa e-mail è fraudolenta, che il pacco non esiste e che l'allegato potrebbe contenere un virus informatico.

Non aprire l'allegato. Questa e-mail e il relativo allegato non provengono da DHL.

Phishing

Il nome DHL è stato usato in numerose attività online fraudolente che vengono definite "Phishing". Una e-mail di questo tipo comunica che DHL sta tentando di consegnare un pacco e chiede al destinatario di aprire l'allegato per poter effettuare la consegna. Questo tipo di e-mail non sono autorizzate da DHL: i mittenti stanno solo usando il nome DHL nel loro messaggio per attirare l'attenzione dell'utente e conferire all'e-mail una apparente legittimità.

DHL raccomanda di non aprire e-mail "provenienti" da DHL, in uno o più dei seguenti casi:

- L'e-mail ricevuta è priva di numero di tracciabilità e non hai nessun rapporto commerciale con DHL
- L'e-mail contiene un allegato e, a quanto ti risulta, non hai nessun rapporto commerciale con DHL
- L'e-mail ti indica di aprire un allegato per conoscere il numero di tracciabilità

Il destinatario di un'e-mail sospetta contenente un "numero di tracciabilità" può sempre verificare sul nostro sito se questo numero è valido. Se la ricerca del numero di tracciabilità non produce risultati, il numero non è valido e l'e-mail che lo contiene non è stata inviata da DHL.

Controlla ora la tracciabilità

Grazie per l'attenzione

Per seguire l'innovazione nella PA:

www.sinetinformatica.it

www.sinetinformatica.it/twitter

www.sinetinformatica.it/facebook