Questo documento indica le principali caratteristiche che attualmente si riscontrano nelle cosiddette mail di phishing/spam che a volte eludono i controlli degli appositi servizi di sicurezza.

- Il testo della mail è spesso in inglese oppure in un italiano con diversi errori grammaticali

- La mail del mittente è decisamente "strana" (es. Luigi Rossi luigi.rossi@yoppuw.ch oppure Luigi Rossi wxbgruyt@lufr.com)

- La mail contiene un allegato spesso zippato, a volte protetto da password (la password è poi indicata nella mail). I files protetti da password non possono essere scansionati dagli antivirus. Può contenere ovviamente anche allegati di altro formato, vale sempre la regola di verificare il mittente ed il testo del messaggio prima di aprire eventuali files contenuti

- La mail contiene un link spesso accompagnato da un invito a collegarsi con credenziali o scaricare files

- Il testo non è pertinente (es. foto delle vacanze, ricette di dolci) oppure non è il tipo di contenuto/richiesta che ci si aspetta da quel mittente

L'elenco soprastante **non può essere esaustivo** in quanto le tecniche possono cambiare. Ma eseguire certi controlli preliminari può essere utile per scartare mail palesemente contraffatte.

In caso di dubbi è sempre bene:

Contattare il mittente della mail se possibile e chiedere lumi.

Non interagire ulteriormente con la mail e mandare una richiesta di verifica a ticket@tech2.it.