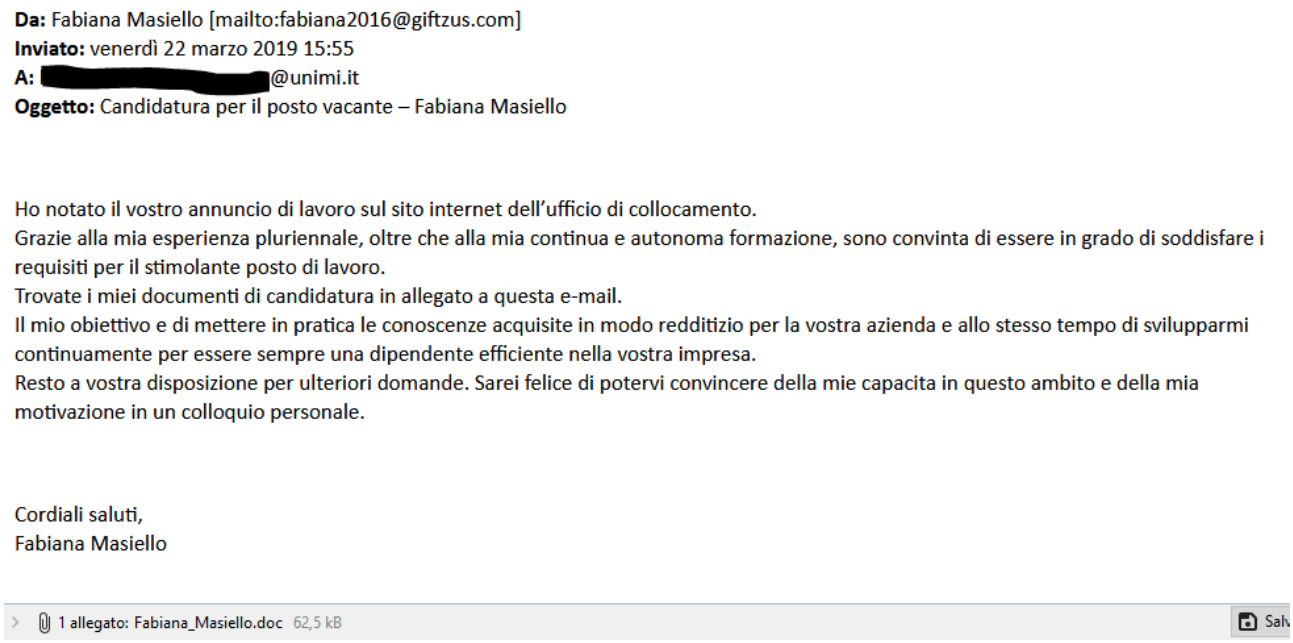
**Campagna di phishing "Candidatura per il posto vacante"**

Gentilissimi utenti,

è attualmente in corso una nuova campagna di malspam, veicolata tramite la posta elettronica, il cui obiettivo è quello di **infettare con un malware il dispositivo dei destinatari.**

Le mail in esame hanno il testo scritto in italiano, e nel testo viene proposta una candidatura per un posto di lavoro. L'allegato è un file in formato .doc**.**

Ecco un esempio di mail:



**Da:** Fabiana Masiello [mailto:fabiana2016@giftzus.com]
**Inviato:** venerdì 22 marzo 2019 15:55
**A:** [redacted]@unimi.it
**Oggetto:** Candidatura per il posto vacante – Fabiana Masiello

Ho notato il vostro annuncio di lavoro sul sito internet dell'ufficio di collocamento.
Grazie alla mia esperienza pluriennale, oltre che alla mia continua e autonoma formazione, sono convinta di essere in grado di soddisfare i requisiti per il stimolante posto di lavoro.
Trovate i miei documenti di candidatura in allegato a questa e-mail.
Il mio obiettivo e di mettere in pratica le conoscenze acquisite in modo redditizio per la vostra azienda e allo stesso tempo di svilupparmi continuamente per essere sempre una dipendente efficiente nella vostra impresa.
Resto a vostra disposizione per ulteriori domande. Sarei felice di potervi convincere della mie capacita in questo ambito e della mia motivazione in un colloquio personale.

Cordiali saluti,
Fabiana Masiello

1 allegato: Fabiana_Masiello.doc 62,5 kB

**Si fa presente che la mail, nel mittente, oggetto e testo, potrebbe presentare alcune modifiche.**

L'Ufficio di Staff Sicurezza ICT invita gli utenti a:

- **non rispondere all'email ricevuta;**
- **non aprire l'allegato.**

**Per coloro i quali abbiano riconosciuto la mail fraudolenta** come sospetta e dunque abbiano ignorato l'email e non abbiano cliccato sul link **non è richiesta alcuna azione**.

**Chiunque avesse erroneamente cliccato e aperto un allegato è invitato a:**

- effettuare una scansione antivirus, e salvare lo screen del risultato
- inviare una email all'Ufficio di Staff Sicurezza ICT all'indirizzo sicurezza@unimi.it, precisando nell'oggetto la campagna di phishing, ed indicando le seguenti informazioni:

1. IP del dispositivo
2. sistema operativo del dispositivo
3. tipo di antivirus in possesso
4. screenshot del risultato della scansione antivirus

Ricordiamo infine che l'Ufficio Sicurezza ICT nella sezione dedicata del portale di Ateneo pubblica:

- **gli avvisi di sicurezza della campagne malevoli in atto al link https://work.unimi.it/servizi/security_gdpr/118606.htm**
- **le linee guida e indicazioni (tra cui quelle per proteggersi dal Phishing) al link https://work.unimi.it/servizi/security_gdpr/118582.htm**

Vi ringraziamo per la collaborazione.

Cordialmente,
Ufficio di Staff Sicurezza ICT