**MODULO PER LA SEGNALAZIONE DI VIOLAZIONI DELLE**

**CREDENZIALI D’ACCESSO AI SERVIZI DELL’ATENEO e/o POSTA ELETTRONICA**

**Obbligatoria ai sensi degli artt. 33 e 34 R. UE. 679/2016**

**Attenzione**: occorre cambiare immediatamente la password utilizzataper la posta istituzionale d’Ateneo seguendo la procedura “se le tue credenziali sono state compromesse” all’indirizzo <https://www.unipg.it/sicurezza-on-line/se-le-tue-credenziali-sono-state-compromesse>. E’ necessario procedere immediatamente a cambiarla anche per i servizi, diversi da quelli dell’Ateneo, nei quali utilizza la stessa password della posta istituzionale.

ll modulo serve per la segnalazione all’Ateneo di eventuali violazioni delle proprie credenziali di accesso ai servizi d’Ateneo, come la posta elettronica di Ateneo.

Le informazioni che fornirà per la segnalazione sono necessari alla stima del problema e alla sua gestione[[1]](#footnote-1): **dovranno pertanto essere il più possibile complete ed esatte,** anche per consentire la corretta stima del danno e provvedere, se del caso, alla comunicazione al Garante[[2]](#footnote-2), se necessaria.

Per lo stesso motivo il presente modulo deve essere trasmesso all’indirizzo [comunicazione.violazione@unipg.it](mailto:comunicazione.violazione@unipg.it) il più tempestivamente possibile, anche da e-mail privata.

In caso di problemi nel procedere secondo tali indicazioni, contatti cortesemente i numeri 075 585 2192 o 2030 dell’ufficio del Responsabile protezione dati.

I dati personali che comunicherà saranno utilizzati solo a tale scopo come da informativa pubblicata all’indirizzo[**INFORMATIVE**](https://www.unipg.it/protezione-dati-personali/informative)**.**

1. **Dati di contatto per eventuali ulteriori informazioni e per la risposta:**

nome e cognome:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

indirizzo e-mail istituzionale o privato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Come è venuto a conoscenza della violazione:

* Ho ricevuto almeno un'email di Microsoft che mi segnala di non aver potuto consegnare una o più email, invii non effettuati da me
* Ho ricevuto almeno una segnalazione, da altri utenti, di email di phishing inviate con il mio account
* Ho riscontrato lo spostamento o la cancellazione di un considerevole quantitativo di email dal mio account di posta
* Ho avuto evidenza di un accesso illegittimo effettuato sui dati gestiti dal servizio, come ad esempio l’apertura di email o documenti che risultano già scaricati
* Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Quando è venuto a conoscenza della violazione?**

(gg/mm/aaaa) \_\_\_/\_\_\_/\_\_\_\_\_\_\_ (hh:mm) \_\_\_\_\_:\_\_\_\_\_

1. **Possibili cause della violazione delle proprie credenziali:**

* Risposta ad un’email di phishing
* Possibile comunicazione o conoscenza delle credenziali da parte di persone note (p.e. collaboratori).
* Smarrimento di un supporto che le riportava scritte in chiaro o utilizzo da postazioni internet pubbliche
* Lettura da osservatore nelle vicinanze
* Coincidenza con password utilizzata per altri servizi on line, NON dell’Ateneo
* Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Quando pensa siano state violate le credenziali?**

(gg/mm/aaaa) \_\_\_/\_\_\_/\_\_\_\_\_\_\_ (hh:mm) \_\_\_\_\_:\_\_\_\_\_

1. **Ha provveduto ad azioni per limitare i danni e se si, quali?**

* Ho effettuato il cambio password
* Ho controllato tutti i miei dispositivi con un software antivirus e antimalware
* Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Quale sistema utilizza per l’accesso alla posta? (marcare almeno una opzione)**

* Sito web (webmail Outlook Web Access - OWA)
* Programma installato sul PC (client di posta come Outlook 2016 o Thunderbird)
* App installata sul proprio dispositivo mobile

1. **Descrivere la natura della violazione osservata sui dati presenti nella casella email o su altri servizi autenticati:**

* **Visualizzazione**: i dati sono stati letti da un numero esiguo di destinatari non autorizzati e che non hanno potuto copiarli o duplicarli
* **Comunicazione**: i dati sono stati comunicati a destinatari non autorizzati e identificabili, anche attraverso copia (p.e. errato destinatario in invio email con dati personali, anche di altre persone)
* **Diffusione**: i dati sono stati comunicati a destinatari non autorizzati e in numero non conoscibile (p.e. i dati acceduti sono stati pubblicati su web)
* **Copia**: è stata effettuata una duplicazione dei dati lasciando inalterati i dati sui dispositivi originari
* **Perdita**: i dati, presumibilmente, esistono ancora, ma ne ha perso il controllo o la possibilità di accedervi
* **Alterazione**: i dati sui sistemi originari hanno subìto delle modifiche non autorizzate (p.e. sono stati crittografati da chi ha violato il sistema, cestinati o altro)
* **Cancellazione**: i dati non sono più disponibili sui sistemi e neppure altrove (p.e. rottura di un disco o pc del quale non esistevano copie di backup)
* **Furto**: i dati non sono più disponibili sui sistemi personali ma sono in possesso di un Terzo
* **Altro**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Quali sono le categorie di interessati cui afferiscono i dati personali contenuti nelle email e/o allegati oggetto della violazione:**

* Studenti
* Personale (di qualsiasi ruolo)
* Collaboratori
* Fornitori
* Forniti da Enti esterni, altri organismi pubblici o privati
* Altro: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **E’ possibile che siano stati acceduti dati che possano comportare furto d’identità, perdite economiche, violazione di segreti d’ufficio o dati afferenti la salute (referti, diagnosi, …), la sfera sessuale o politica, fotografie, documenti contenenti dati potenzialmente pericolosi se utilizzati malevolmente? Se si, darne**

**una descrizione:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Qual è il numero (anche approssimativo) di persone coinvolte dalla violazione (indirizzi in rubrica, numero di messaggi, elementi inseriti nel testo o negli allegati ai messaggi,…):**

* numero \_\_\_\_\_
* fascia numerica (cento o multipli, migliaia,..) : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* al momento non stimabile

1. **Nella rubrica sono presenti numeri di cellulare, indirizzi con i nominativi, oltre**

**l’e-mail? : SI NO**

1. Come previsto dal R.UE. 679/2016, artt.33 e 34 [↑](#footnote-ref-1)
2. La comunicazione, se necessaria, deve essere effettuata dall’Ateneo entro le 72h previste dal Regolamento UE [↑](#footnote-ref-2)