- **Oggetto:** ATTENZIONE - INVIO FALSE E-MAIL CONTENENTI ALLEGATI DANNOSI
- **Data ricezione email:** 23/03/2018 10:26
- **Mittenti:** MIUR - NO REPLY - Gest. doc. - Email: noreply@istruzione.it
- **Indirizzi nel campo email 'A':** <scuole-nazionale@istruzione.it>
- **Indirizzi nel campo email 'CC':**
- **Indirizzo nel campo 'Rispondi A':** <noreply@istruzione.it>

Testo email

Come segnalatoci dal CERT-Pubblica Amministrazione, vi avvisiamo che nelle ultime ore si sta diffondendo nel nostro Paese una nuova massiccia campagna di phishing che mira ad infettare il PC delle vittime.

Le E-mail fraudolente sembrano provenire da mittenti italiani, sono scritte in lingua italiana, e contengono in allegato un file Word che in molti casi è denominato “XYX_Richiesta.doc” (con XYZ variabile), contenente al suo interno una Macro malevola.

L’oggetto e il testo dell’email, così come il nome dell’allegato, potrebbero variare a seconda del destinatario.

Al fine di arginare il fenomeno, come sempre, si raccomanda di:

- non cliccare su link “sospetti”: non farsi ingannare dal nome del link ma visualizzare l’indirizzo reale del sito passando - senza cliccare - col mouse sul link.
- non aprire file “sospetti”
- cestinare le e-mail “sospette”: ad es. scritte con errori ortografici e grammaticali, in un italiano stentato, con richiesta di inserire PIN, password e dati personali su una pagina web
- effettuare frequentemente il backup dei dati presenti sulla propria postazione, al fine di evitare la perdita degli stessi
- procedere comunque ad un costante aggiornamento del proprio antivirus

In caso di infezione, spegnere o disconnettere immediatamente il computer dalla rete, ed eventuali dispositivi ad esso collegati: quindi contattare l’assistenza tecnica.

Ministero dell'Istruzione, dell'Università e della Ricerca

D.G. Contratti, Acquisti, Sistemi Informativi e Statistica