Spam in the 21st Century

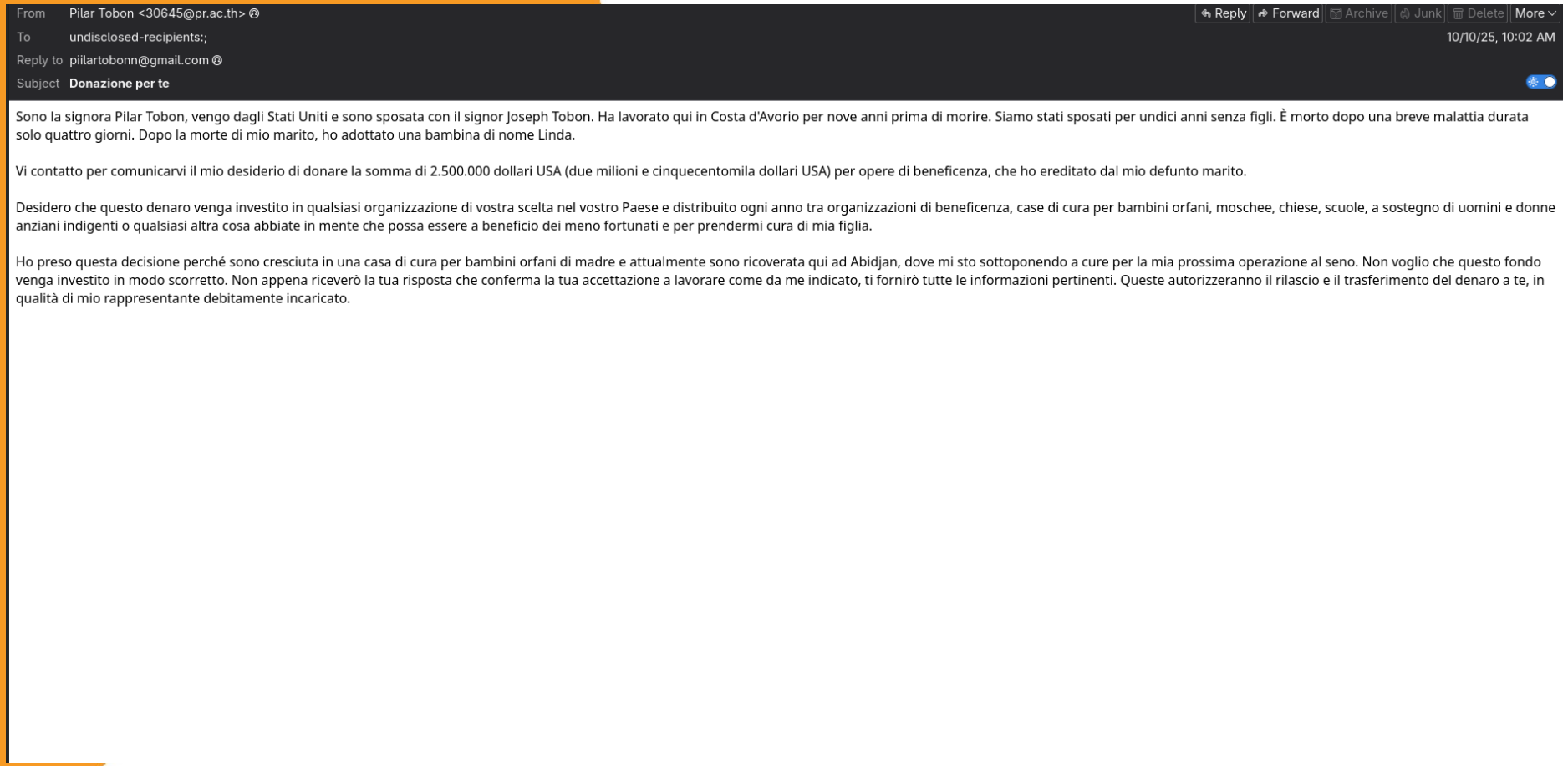
The Battle Between Attack and Defense

Giovanni Bechis
<gbechis@apache.org>

How an antispam software works

- Ocr, attachment checks and qr-codes detection
- Text analysis
- Links analysis
- Real time blacklists
  - Domains
  - Ip addresses
  - Email addresses
  - BTC wallets
  - Phone numbers
  - Esp accounts
- A.I.

Simple spam messages



From Pilar Tobon <30645@pr.ac.th>
To undisclosed-recipients:;
Reply to piilartobonn@gmail.com
Subject **Donazione per te**

Reply Forward Archive Junk Delete More
10/10/25, 10:02 AM

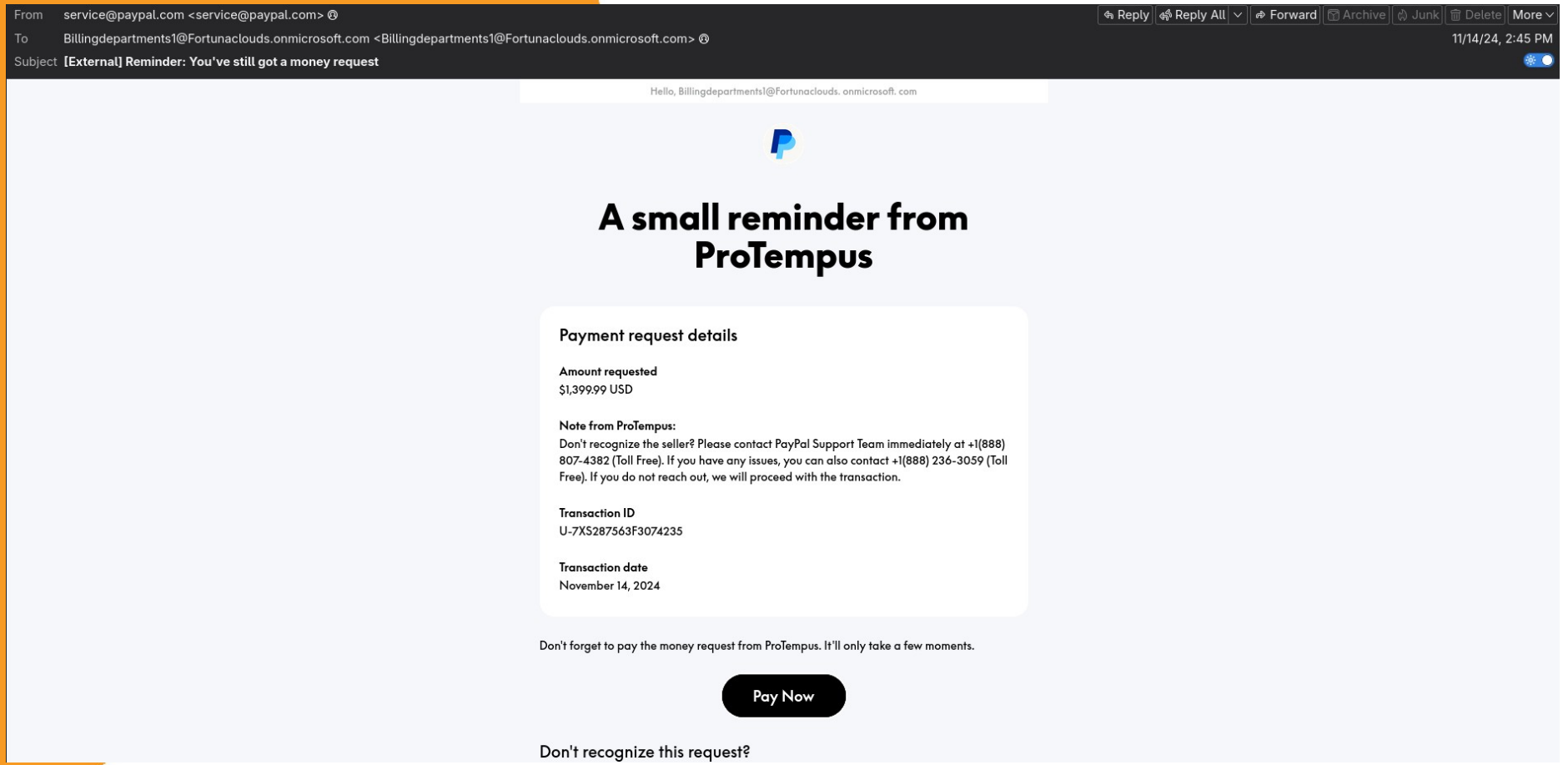
Sono la signora Pilar Tobon, vengo dagli Stati Uniti e sono sposata con il signor Joseph Tobon. Ha lavorato qui in Costa d'Avorio per nove anni prima di morire. Siamo stati sposati per undici anni senza figli. È morto dopo una breve malattia durata solo quattro giorni. Dopo la morte di mio marito, ho adottato una bambina di nome Linda.

Vi contatto per comunicarvi il mio desiderio di donare la somma di 2.500.000 dollari USA (due milioni e cinquecentomila dollari USA) per opere di beneficenza, che ho ereditato dal mio defunto marito.

Desidero che questo denaro venga investito in qualsiasi organizzazione di vostra scelta nel vostro Paese e distribuito ogni anno tra organizzazioni di beneficenza, case di cura per bambini orfani, moschee, chiese, scuole, a sostegno di uomini e donne anziani indigenti o qualsiasi altra cosa abbiate in mente che possa essere a beneficio dei meno fortunati e per prendermi cura di mia figlia.

Ho preso questa decisione perché sono cresciuta in una casa di cura per bambini orfani di madre e attualmente sono ricoverata qui ad Abidjan, dove mi sto sottoponendo a cure per la mia prossima operazione al seno. Non voglio che questo fondo venga investito in modo scorretto. Non appena riceverò la tua risposta che conferma la tua accettazione a lavorare come da me indicato, ti fornirò tutte le informazioni pertinenti. Queste autorizzeranno il rilascio e il trasferimento del denaro a te, in qualità di mio rappresentante debitamente incaricato.

Complex spam messages



QR-CODES

From Summer Consultants@Netsuite.Scanner <admin@cabram.com>
To [redacted]
Subject [External] [redacted]-CSV Import- EMA Contract Invoice:Sign&ReturnFriday October 2023.

Reply | Reply All | Forward | Archive | Junk | Delete | More

10/14/23, 12:37 AM

DocuSign

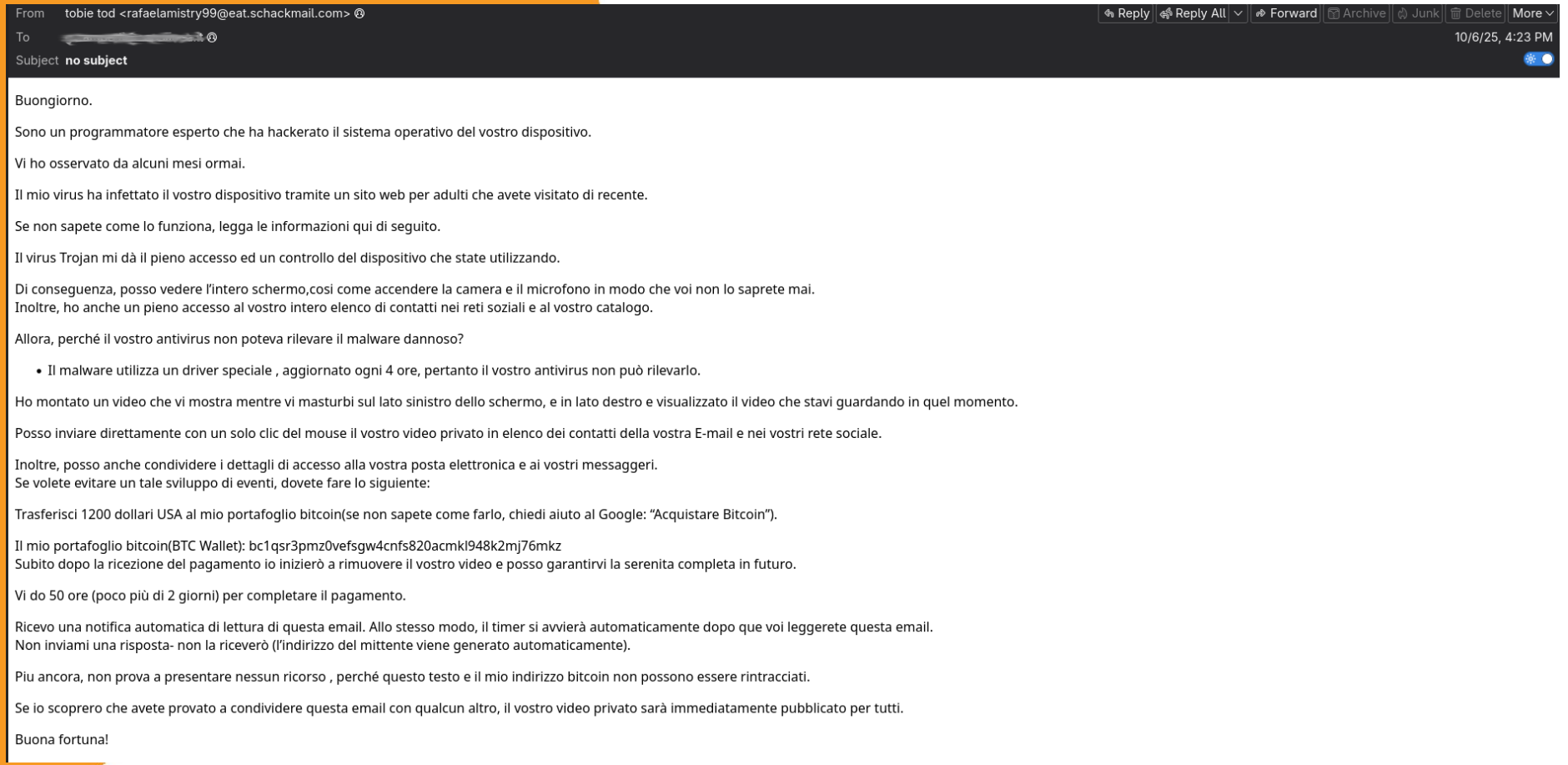
You have received a new document to review and sign

To review, scan the QR code above.

All parties have completed Complete with DocuSign: doc20230516211407.pdf.

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Bitcoin scam



From tobie tod <rafaelamistry99@eat.schackmail.com>
To [redacted]
Subject **no subject**

Reply | Reply All | Forward | Archive | Junk | Delete | More

10/6/25, 4:23 PM

Buongiorno.

Sono un programmatore esperto che ha hackerato il sistema operativo del vostro dispositivo.

Vi ho osservato da alcuni mesi ormai.

Il mio virus ha infettato il vostro dispositivo tramite un sito web per adulti che avete visitato di recente.

Se non sapete come lo funziona, legga le informazioni qui di seguito.

Il virus Trojan mi dà il pieno accesso ed un controllo del dispositivo che state utilizzando.

Di conseguenza, posso vedere l'intero schermo,cosi come accendere la camera e il microfono in modo che voi non lo saprete mai.
Inoltre, ho anche un pieno accesso al vostro intero elenco di contatti nei reti soziali e al vostro catalogo.

Allora, perché il vostro antivirus non poteva rilevare il malware dannoso?

- Il malware utilizza un driver speciale , aggiornato ogni 4 ore, pertanto il vostro antivirus non può rilevarlo.

Ho montato un video che vi mostra mentre vi masturbi sul lato sinistro dello schermo, e in lato destro e visualizzato il video che stavi guardando in quel momento.

Posso inviare direttamente con un solo clic del mouse il vostro video privato in elenco dei contatti della vostra E-mail e nei vostri rete sociale.

Inoltre, posso anche condividere i dettagli di accesso alla vostra posta elettronica e ai vostri messaggeri.
Se volete evitare un tale sviluppo di eventi, dovete fare lo siguiente:

Trasferisci 1200 dollari USA al mio portafoglio bitcoin(se non sapete come farlo, chiedi aiuto al Google: "Acquistare Bitcoin").

Il mio portafoglio bitcoin(BTC Wallet): bc1qsr3pmz0vefsgw4cnfs820acmkl948k2mj76mkz
Subito dopo la ricezione del pagamento io inizierò a rimuovere il vostro video e posso garantirvi la serenita completa in futuro.

Vi do 50 ore (poco più di 2 giorni) per completare il pagamento.

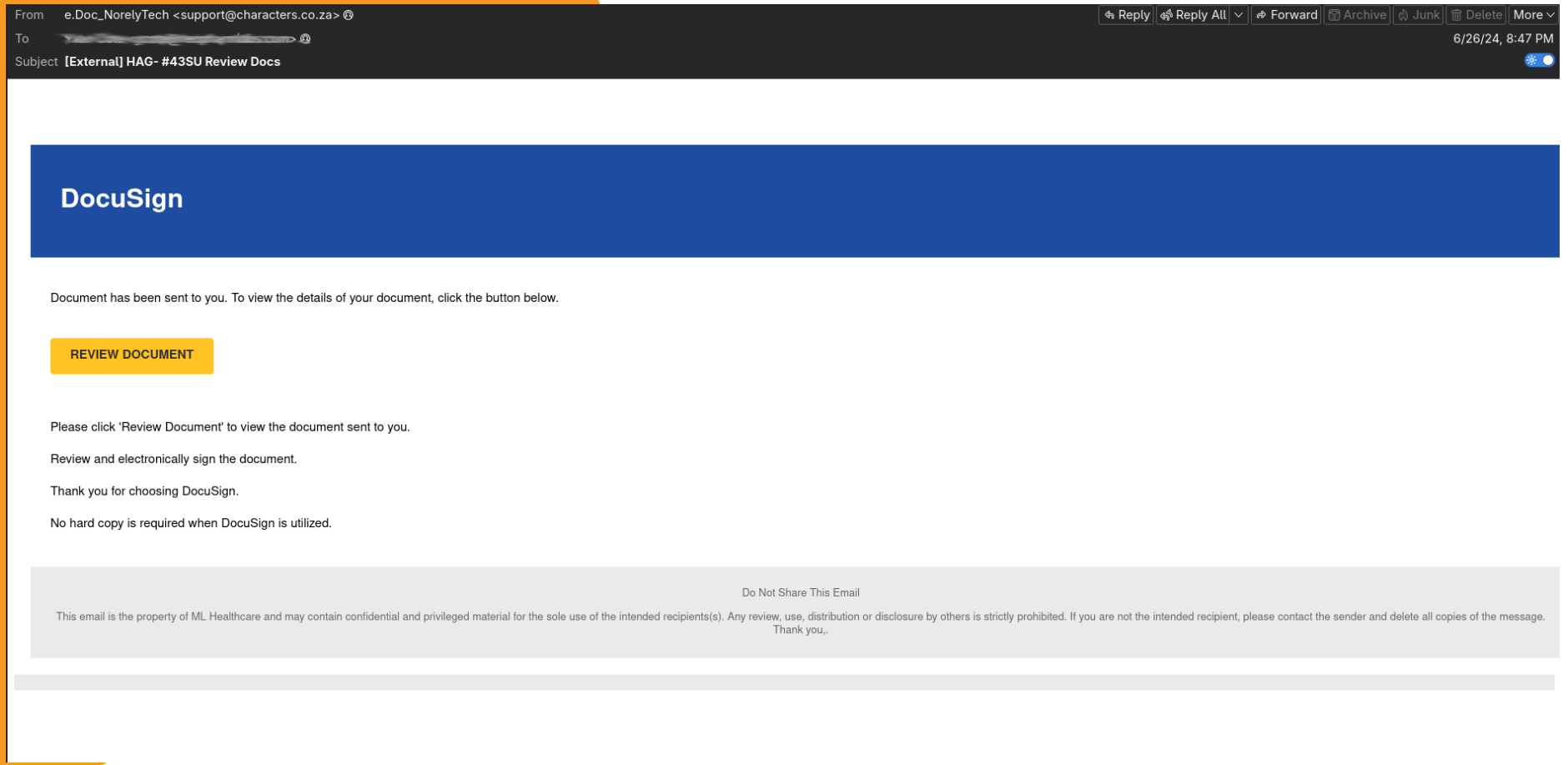
Ricevo una notifica automatica di lettura di questa email. Allo stesso modo, il timer si avvierà automaticamente dopo que voi leggerete questa email.
Non inviami una risposta- non la riceverò (l'indirizzo del mittente viene generato automaticamente).

Piu ancora, non prova a presentare nessun ricorso , perché questo testo e il mio indirizzo bitcoin non possono essere rintracciati.

Se io scoprero che avete provato a condividere questa email con qualcun altro, il vostro video privato sarà immediatamente pubblicato per tutti.

Buona fortuna!

Url Shorteners & Redirectors



From e.Doc_NorelyTech <support@characters.co.za>
To [redacted]
Subject [External] HAG- #43SU Review Docs

Reply | Reply All | Forward | Archive | Junk | Delete | More

6/26/24, 8:47 PM

DocuSign

Document has been sent to you. To view the details of your document, click the button below.

REVIEW DOCUMENT

Please click 'Review Document' to view the document sent to you.

Review and electronically sign the document.

Thank you for choosing DocuSign.

No hard copy is required when DocuSign is utilized.

Redirectors

- https://www.google.com/amp/s/mircosoft.es/www/#WV...
- https://click.pstmrk.it/3s/...%25252Fzs.komivor.ru%2525251/...
- https://www.bing.com/ck/a?!&&p=5f467c7273effecfJmltd...
- https://public-api.wordpress.com/...?redirect_to=http%3A%2F%2Ffrenchitivity.com%2F2024...
- https://login.microsoftonline.com/...?redirect_uri=https%3A%2F%2Fazure.saskaggrads.com

Too big to block abused services

- Google, Microsoft 365 and other freemail providers
- ESPs (Sendgrid, Mailchimp, AmazonSES, Sendinblue, ...)
- Hacked mailing lists

Thanks

Questions ?

Apache SpamAssassin

THE ASF