INTERVENTO

Politecnico di Torino · 6 novembre 2026

L'azione di contrasto della Guardia di Finanza alle più avanzate truffe nell'era della governance digitale

Cap. Davide Luzi
Nucleo di Polizia Economico-Finanziaria Torino
Comandante Sezione Altra Criminalità Economica

Struttura dell'intervento

Oggi risponderemo a tre domande:

1

Come si sono evolute le frodi telematiche in ambito aziendale e professionale?

2

Quali rischi emergono dall'Intelligenza Artificiale e dalle «truffe moderne»?

3

Come agisce concretamente la Guardia di Finanza a tutela del tessuto economico?

La matrice giuridica

ART. 640 CODICE PENALE

«Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno.»

La norma è invariata

Cambia la natura degli artifizi e dei raggiri.

Nel contesto digitale, il raggiro non sfrutta più solo l'ingenuità del singolo privato ma punta a violare i processi di verifica e la catena di fiducia delle imprese.

La porta d'ingresso

Guardia di Finanza

80%+

degli attacchi informatici rivolti al mondo business parte da phishing, smishing e spoofing.

Phishing e Smishing:

Messaggi ingannevoli via mail o sms che simulano ad esempio comunicazioni bancarie.

> *«Gentile cliente, si è verificata un'anomalia sul suo conto. Clicchi qui per verificare.»*

Spoofing: falsificare l’identità del mittente

Tecnica utilizzata per alterare il reale numero di telefono, SMS o indirizzo e-mail al fine di ingannare l’utente ricevente.
L'SMS truffa si inserisce nella stessa chat storica e autentica della banca, ingannando anche la persona più cauta.

Phishing privato vs Phishing aziendale

Guardia di Finanza

Phishing privato

«Pesca a strascico»

Messaggio generico inviato a milioni di utenti, sperando che qualcuno abbocchi.

Phishing aziendale

«Caccia di precisione» (spear phishing)

L'attacco è studiato nei minimi dettagli per una specifica impresa: profili LinkedIn, organigramma, fornitori, contratti in corso.

Man-in-the-Middle

1 I truffatori hackerano l'email aziendale → **2** Intercettano la fattura modificando l'IBAN → **3** L'azienda paga in buona fede

Indicatori e difese

Guardia di Finanza

!

Segnali d'allarme

- Cambio IBAN dell'ultimo minuto
- Dominio e-mail con lievi difformità (spoofing e-mail)
- IBAN esteri o di carte ricaricabili

OOB

Verifica fuori banda

Mai rispondere alla mail né usare i contatti in firma: chiamare il referente su un canale autonomo (rubrica o contratto).

VOP

Verification of Payee

Se la banca segnala una mancata corrispondenza tra denominazione sociale e titolare dell'IBAN, blocca l'operazione.

L'evoluzione della truffa con l'I.A.

Guardia di Finanza

Phishing iper-personalizzato

Niente più errori grammaticali: i modelli generativi scrivono in perfetto italiano formale, imitando lo stile della direzione finanziaria.

Voice spoofing (deepfake vocale)

Bastano pochi secondi di audio, da un intervento, un podcast o un video LinkedIn, per clonare la voce di un amministratore delegato.

Caso reale: ex presidente di Fideuram, ha effettuato bonifici per 95 milioni di euro autorizzati dopo un messaggio attribuito al CEO di Intesa Sanpaolo e una telefonata con voce clonata.

Il Deepfake

«Vedere con i propri occhi (NON) è la prova regina della realtà.»

Oggi la tecnologia rende estremamente difficile distinguere la realtà dalla finzione.



Guardia di Finanza

Truffe moderne: finta I.A.

Guardia di Finanza

La promessa

Un fornitore si presenta in azienda proponendo una piattaforma d'avanguardia che gestisce con I.A. i dati aziendali riservati.

La realtà

L'azienda venditrice non possiede alcuna I.A. proprietaria: i documenti finiscono su server non protetti o servizi pubblici non autorizzati.

Il risultato

Frode commerciale (l'azienda paga una tecnologia inesistente) e data breach (violazione dei dati).

Truffe moderne: Green AI

Guardia di Finanza

Promessa	Un fornitore propone servizi Cloud «a impatto zero» con certificazioni spendibili nel Bilancio di Sostenibilità.
Controlli	Quando la Capofiliera o le banche effettuano i controlli in ottica di compliance e direttiva CSRD, emerge che le dichiarazioni sono prive di fondamento (fake claims).
Conseguenza	Accusa di greenwashing: uscita dalla filiera dei fornitori qualificati, contrazione del credito bancario.

In entrambi i casi l'imprenditore non è stato ingenuo: ha firmato un contratto. La tutela del dato e la scelta dei partner sono tasselli fondamentali della governance aziendale.

Il ruolo della Guardia di Finanza

Guardia di Finanza

Polizia economico-finanziaria + **Polizia giudiziaria**

Azione preventiva, analitica e repressiva

Monitoraggio dei flussi finanziari sospetti e individuazione degli schemi fraudolenti prima che destabilizzino l'economia reale; ricostruzione delle filiere criminali anche quando il denaro transita su circuiti esteri o piattaforme di criptovalute.

L'articolazione operativa del Corpo

1

Reparti territoriali

Presenza capillare sul territorio: contatto diretto con cittadini e imprese e ricezione tempestiva delle notizie di reato.

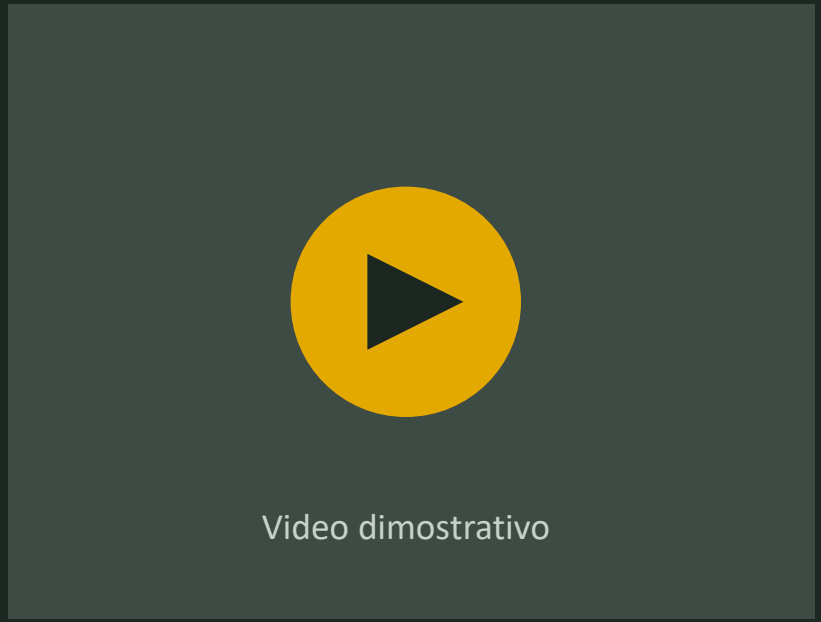
2

Reparti speciali

Dal 2001 il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche: alta specializzazione tecnica a supporto delle operazioni cibernetiche più complesse.

Esperimento sociale

«Prima di concludere, desidero condividere con voi un breve video.»



Responsabilità condivisa

Formazione	Procedure di controllo	Consapevolezza

Le informazioni che pubblichiamo sono la materia prima della truffa perfetta.

La Guardia di Finanza farà rigorosamente la propria parte.
A ciascuno di noi spetta il compito di fare la propria.

Grazie per l'attenzione