TRUST aWARE

FONDAZIONE Mondo Digitale

Enhancing Digital Security, Privacy and TRUST in softWARE

Come Evitare le Truffe Online

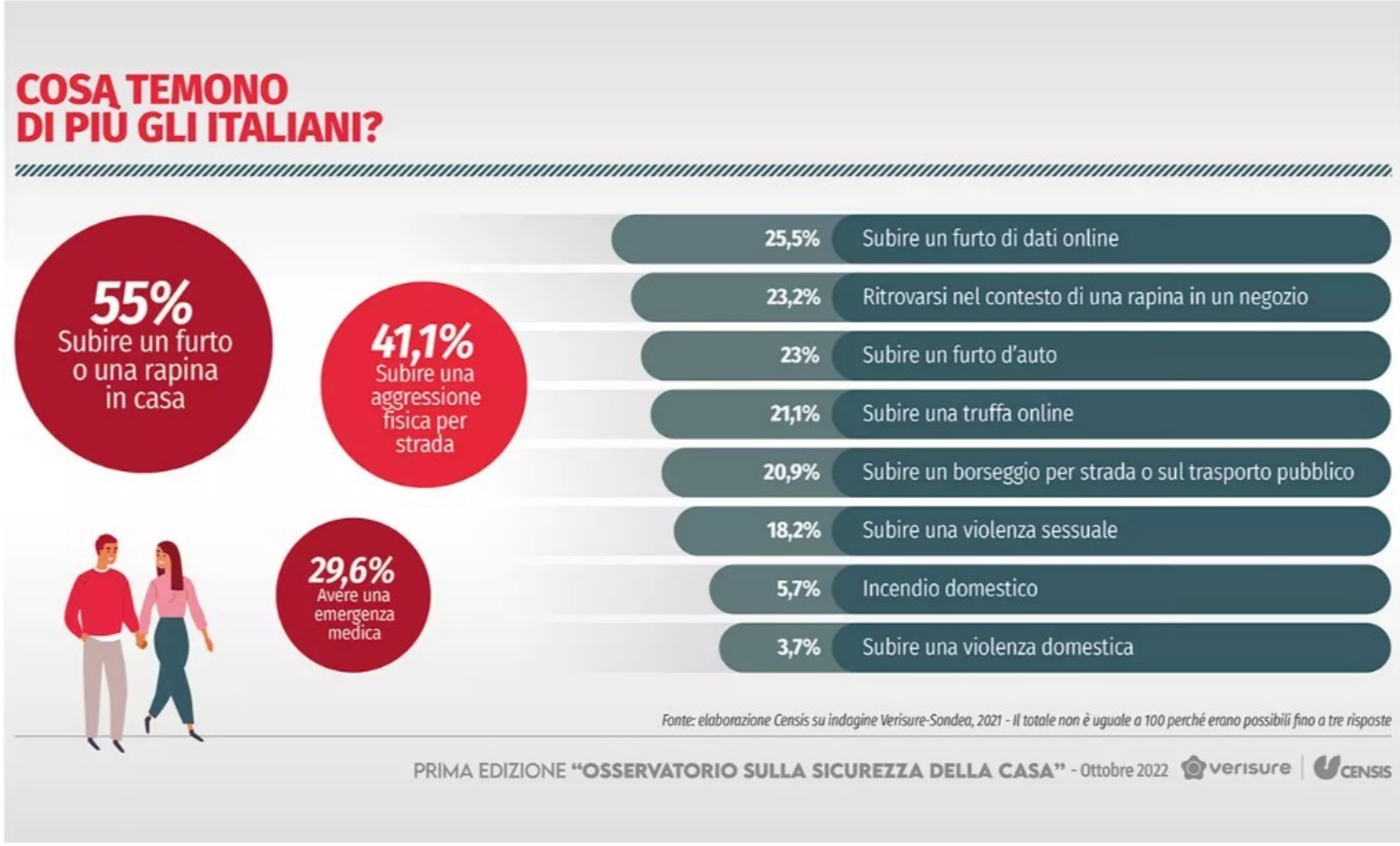
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

TRUST aWARE

FONDAZIONE Mondo Digitale

Index

Cosa Temono Gli Italiani - 2022



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Le Truffe Online Più Comuni - 2022

Le tipologie di truffe più frequenti online:

1. **E-Mail**: riguardano problematiche legate a conti correnti e/o bancari, spedizioni, pagamenti, finte notifiche di avvocati/notai, per l'estorsione dei dati di accesso

2. **Siti Istituzionali**: INPS, Agenzia delle Entrate, Agenzia delle Riscossioni, Banche e Poste Italiane sono tra i più replicati con fini di furto delle credenziali di accesso

3. **Siti di E-Commerce Internazionali con vendita e spedizione veloce**: messa online di numerose landing page quasi identiche al sito originale con cui carpire dati sensibili e di pagamento (Amazon, eBay, ecc…)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Le Truffe Online

Le truffe online sono una tecnica di cyber attacco che ha come scopo finale quello di impossessarsi delle credenziali, dell'identità o dei dati sensibili di un utente.

Attraverso le truffe online l'utente subisce una manipolazione dovuta ad una realizzazione, pressoché identica all'originale, di e-mail, landing page e notifiche di urgenza.

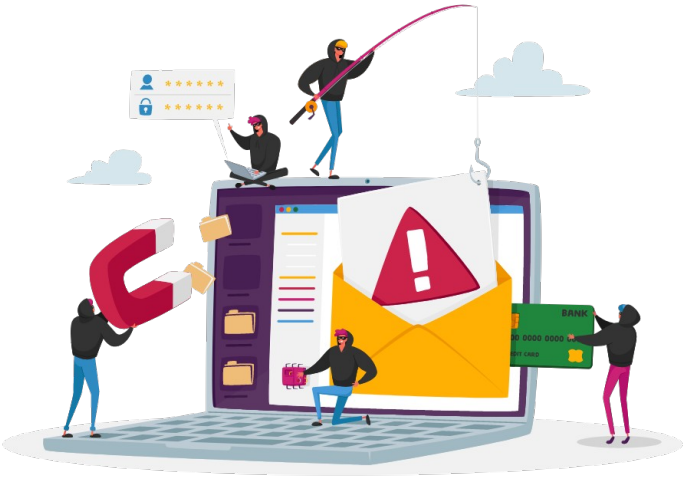
Una delle tecniche più conosciute per i furti online è il **Phishing**.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Phishing

La parola **Phishing** è una variazione ortografica della parola *fishing* (dall'inglese to fish = pescare).

Il Phishing avviene quando un hacker manipola le informazioni digitali per far credere all'utente che l'azione che sta per compiere sia sicura e assolutamente normale.



L'esca è spesso una e-mail, un SMS, un messaggio su una chat online come Messenger o WhatsApp, una landing page oppure un form di contatto che si trova cliccando su un link.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Phishing

Cosa sfrutta l'hacker per mette in atto la pratica del phishing

1. Utilizza loghi o nomi molto simili all'originale (solo un occhio allenato e attento potrebbe cogliere le diversità)

2. Sfrutta leve psicologiche forti (paura, eccitazione, emozione) e agisce in orari particolari della giornata (appena svegli, pomeriggio in pieno orario lavorativo, sera tardi quando siamo stanchi, ecc)

3. Utilizza un link credibile (una i maiuscola al posto della l minuscola in un link può passare facilmente inosservata)

4. Utilizza una Call-To-Action (= invito all'azione) forte e urgente

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Phishing

Cosa esaminare quando riceviamo un messaggio sospetto

- **Mittente**: è un indirizzo e-mail, un numero o un nome utente che conosciamo?
- **Grammatica e ortografia**: la forma utilizzata per la scrittura dell'e-mail o del SMS è corretta? Modi e tempi verbali sono rispettati? Sembra riprodurre una traduzione molto approssimativa?
- **Personalizzazione assente**: saluti e destinatari del messaggio saranno vaghi e impersonali

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Phishing

- **Peculiarità del brand**: il logo o il font utilizzato corrispondono a quelli del brand reale?
- **Formattazione del testo**: ci sono parti di testo scritte con font di dimensioni maggiori e altri di dimensioni minori? E il colore del testo è sempre lo stesso?
- **Oggetto dell'e-mail**: assente oppure contenente caratteri in grassetto, punteggiatura ripetuta più volte (!!!!! - ????)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Esempi di Phishing

Messaggio impersonale: dettagli del destinatario non presenti

Testo del messaggio: grammaticalmente poco corretto

Link cliccabile: istituti di credito e Poste Italiane non inviano link cliccabili nelle comunicazioni

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Esempi di Phishing

Da: news <admin@pc-mediation.com>
Inviato:
A:
Oggetto: Licenza 534238623
Allegati: inform_1852.zip

Agenzia Entrate

Direzione Centrale Gestione Tributi

Gentile contribuente,
dall'esame dei fatti e dei versamenti relativi alla Comunicazione delle liquidazioni periodiche Iva, da voi mostrata per l'ultimo trimestre 2020, sono emerse alcune incoerenze.
Le informazioni relative alle incoerenze sono visionabili nel documento in allegato o nel "Cassetto fiscale" (sezione L'Agenzia scrive) e nel servizio "Fatture e Corrispettivi (sezione Consultazione - L'Agenzia scrive),
entrambi accessibili dal sito web dell'Agenzia delle entrate (www.agenziaentrate.gov.it).

Password: gov2021

Questa e-mail è stata figliata automaticamente, pertanto la preghiamo di non reagire a questo indirizzo di posta elettronica.

Destinatario: indirizzo e-mail non di dominio e poco coerente con l'organo che rappresenta

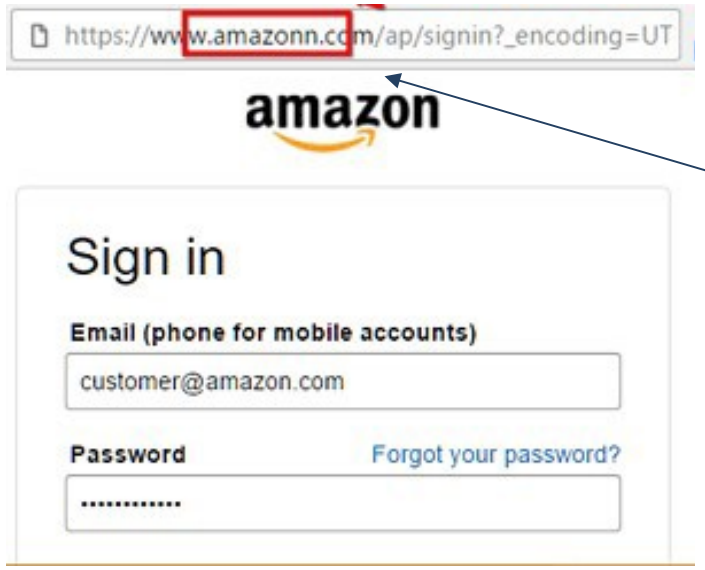
Messaggio impersonale: dettagli del destinatario non presenti

Testo: grammaticalmente non corretto, con forme di cortesia errate

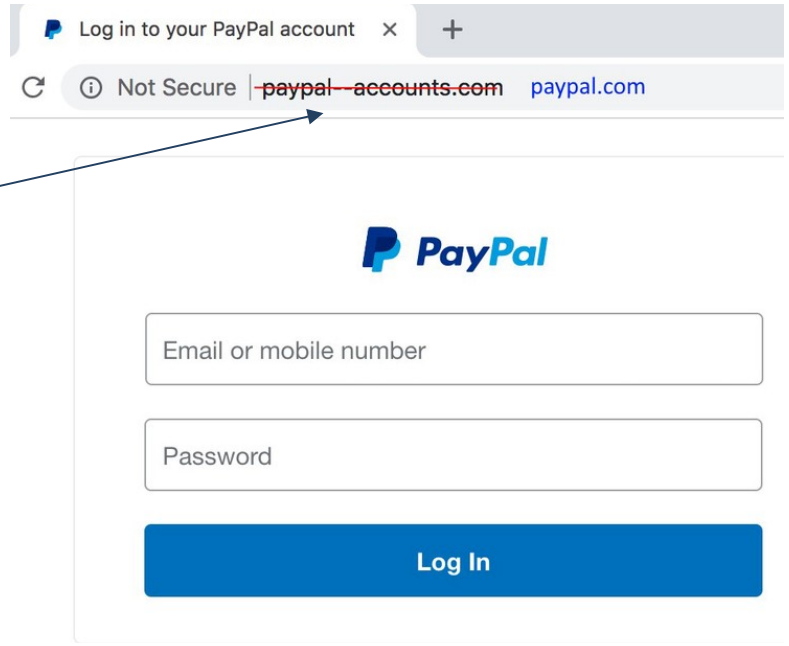
Traduzione imprecisa

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Esempi di Phishing



Impostazione grafica identica
MA
URL differente che rimanda ad un dominio non ufficiale



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Spear Phishing

Lo **Spear Phishing** è una truffa online mirata e diretta ad una sola persona.

Lo si attua per mettere a segno un furto di identità o di dati sensibili e personali specifici.

La vittima viene prescelta e la truffa online viene costruita in base alle sue abitudini e conoscenze.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Spear Phishing

Cosa sfrutta l'hacker per mette in atto la pratica dello spear phishing

1. Utilizza nomi o brand che la vittima contatta regolarmente

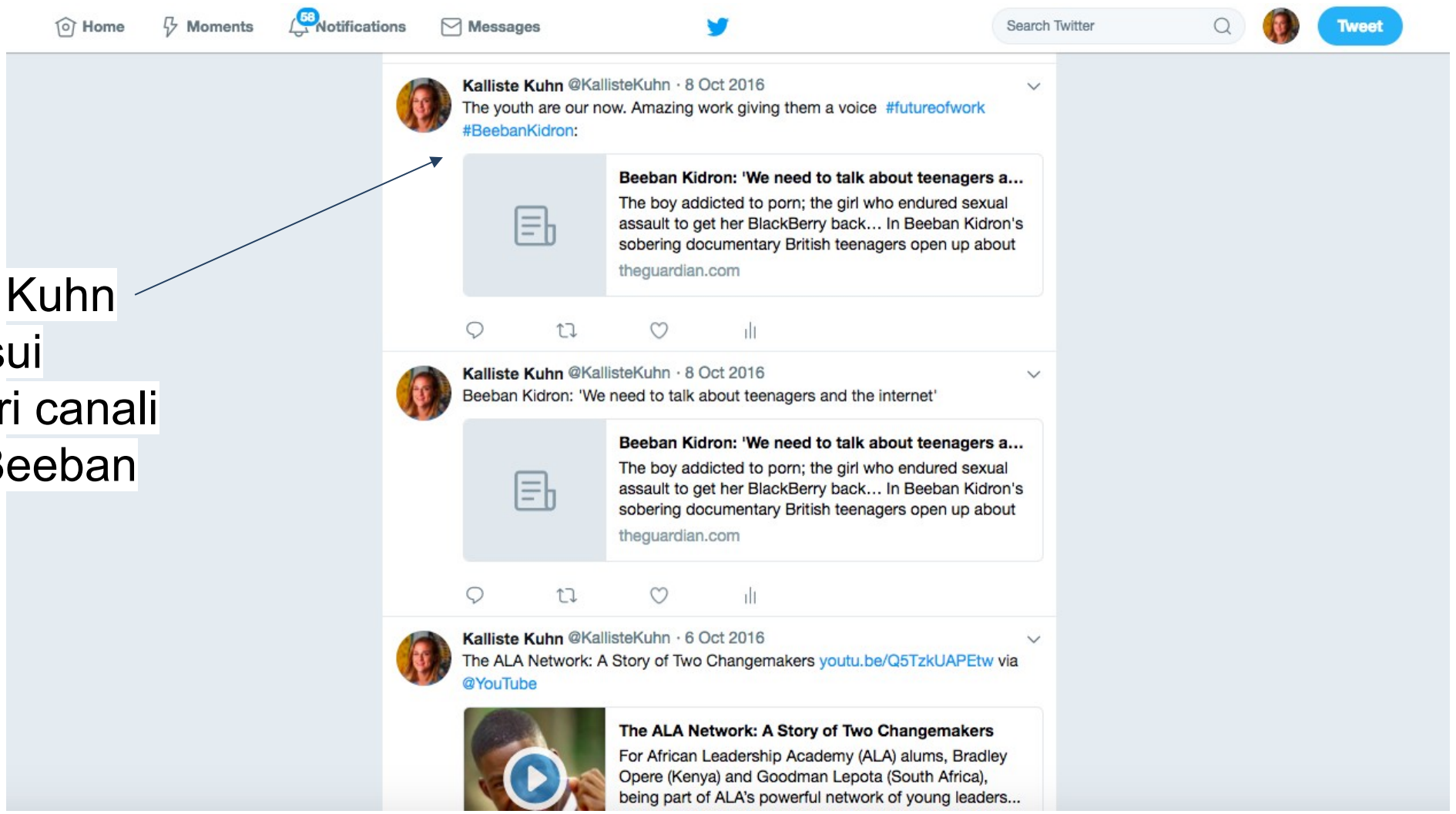
2. Crea una e-mail, un messaggio esca che convinca l'utente a fidarsi nel fare l'azione richiesta

3. Utilizza un link credibile/una landing page identica all'originale per reperire le informazioni sensibili di cui ha bisogno

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Spear Phishing: il caso studio Kalliste Kuhn

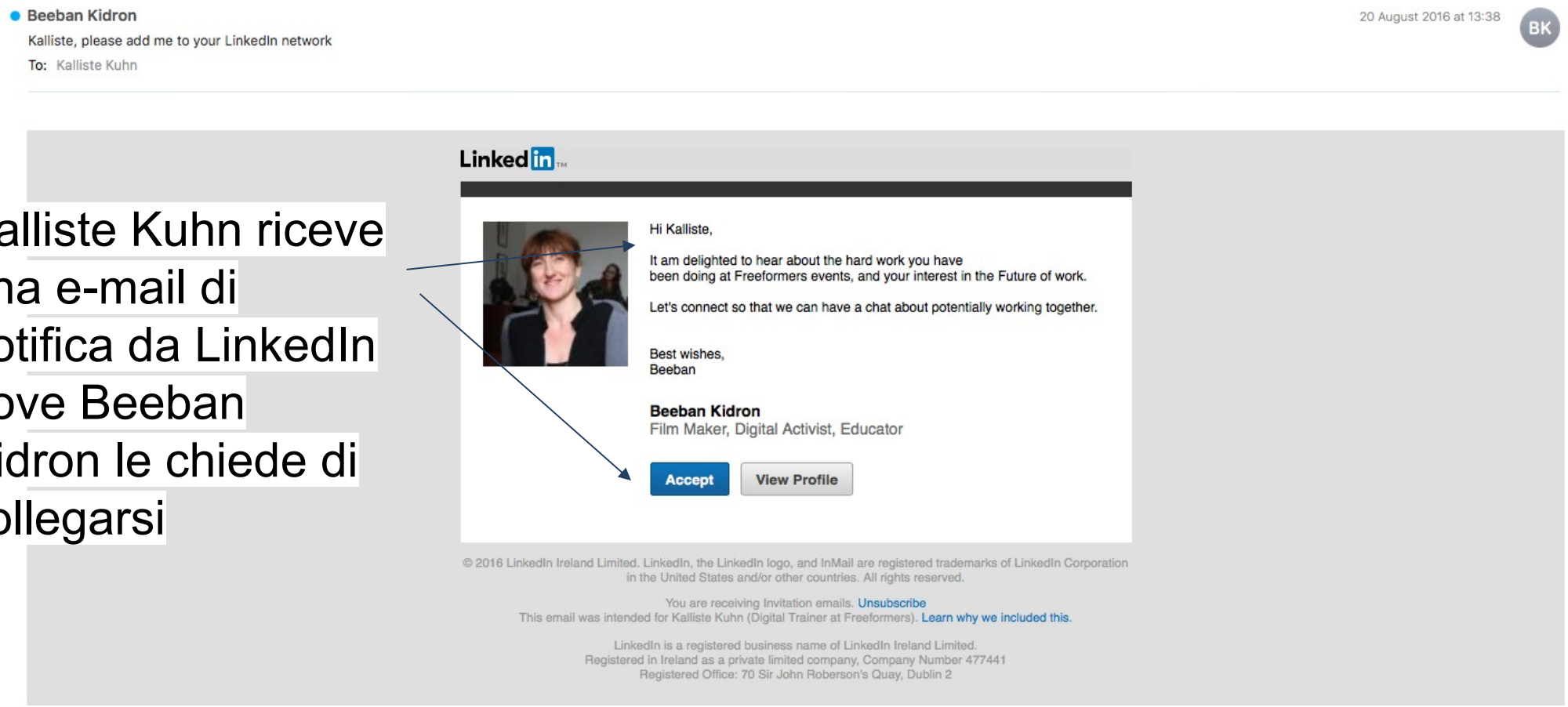
Kalliste Kuhn segue sui maggiori canali social Beeban Kidron



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Spear Phishing: il caso studio Kalliste Kuhn

Kalliste Kuhn riceve una e-mail di notifica da LinkedIn dove Beeban Kidron le chiede di collegarsi



Beeban Kidron
Kalliste, please add me to your LinkedIn network
To: Kalliste Kuhn

20 August 2016 at 13:38 BK

LinkedIn

Hi Kalliste,

It am delighted to hear about the hard work you have been doing at Freeformers events, and your interest in the Future of work.

Let's connect so that we can have a chat about potentially working together.

Best wishes,
Beeban

Beeban Kidron
Film Maker, Digital Activist, Educator

Accept View Profile

© 2016 LinkedIn Ireland Limited. LinkedIn, the LinkedIn logo, and InMail are registered trademarks of LinkedIn Corporation in the United States and/or other countries. All rights reserved.

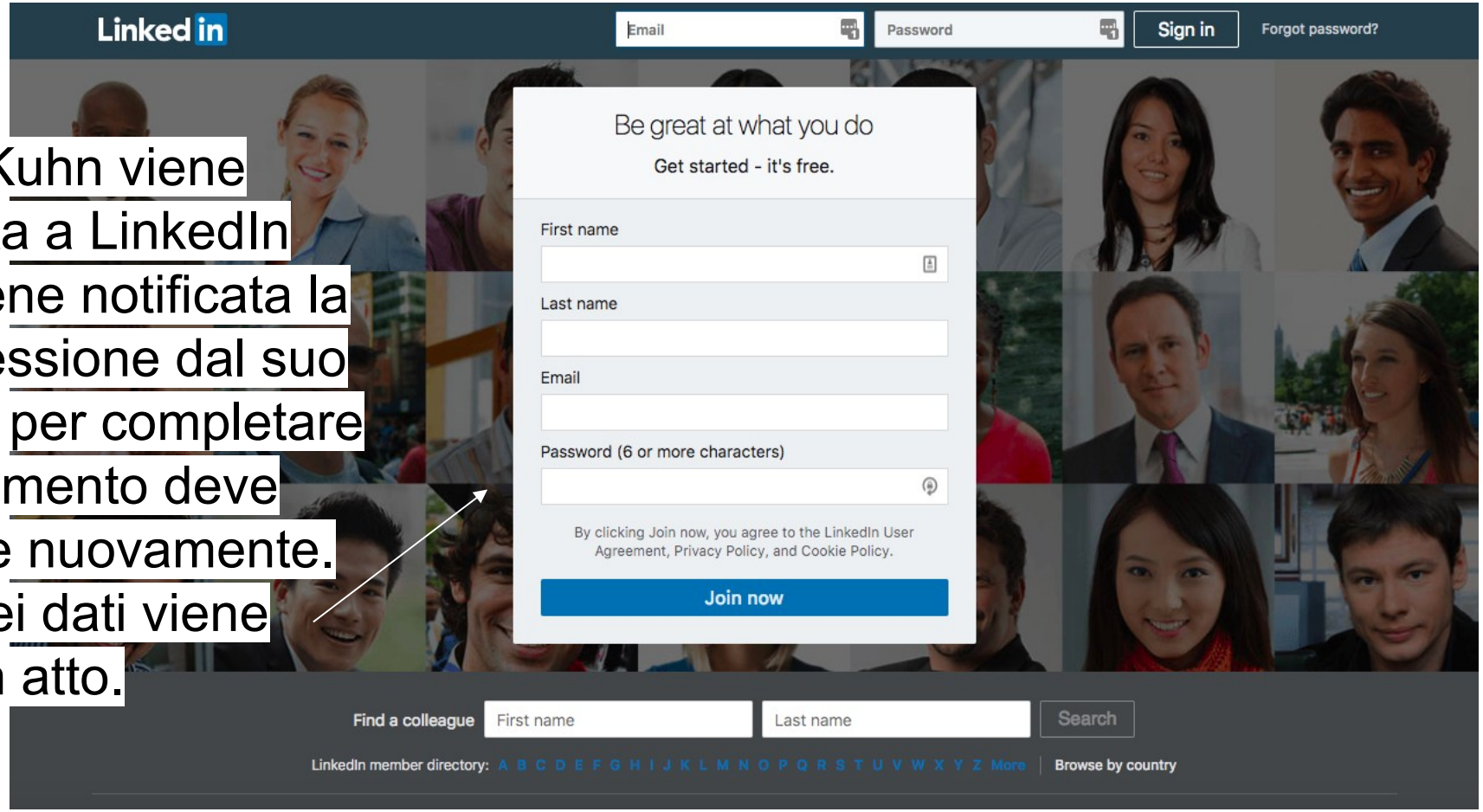
You are receiving Invitation emails. Unsubscribe
This email was intended for Kalliste Kuhn (Digital Trainer at Freeformers). Learn why we included this.

LinkedIn is a registered business name of LinkedIn Ireland Limited.
Registered in Ireland as a private limited company, Company Number 477441
Registered Office: 70 Sir John Roberson's Quay, Dublin 2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Spear Phishing: il caso studio Kalliste Kuhn

Kalliste Kuhn viene rimandata a LinkedIn ma le viene notificata la disconnessione dal suo account, per completare il collegamento deve accedere nuovamente. Il furto dei dati viene messo in atto.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Whaling

Il **Whaling** è simile allo Spear Phishing ma punta specificamente a dirigenti, CEO, imprenditori di livello.

L'hacker sfrutta

1. Una situazione di estrema urgenza e potenzialmente pericolosa a livello amministrativo - burocratico - economico

2. Una e-mail in cui viene intimata una comunicazione urgente a cui far seguito con una video call cliccando su un link o con la compilazione di documenti urgenti attraverso il download degli allegati

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Smishing

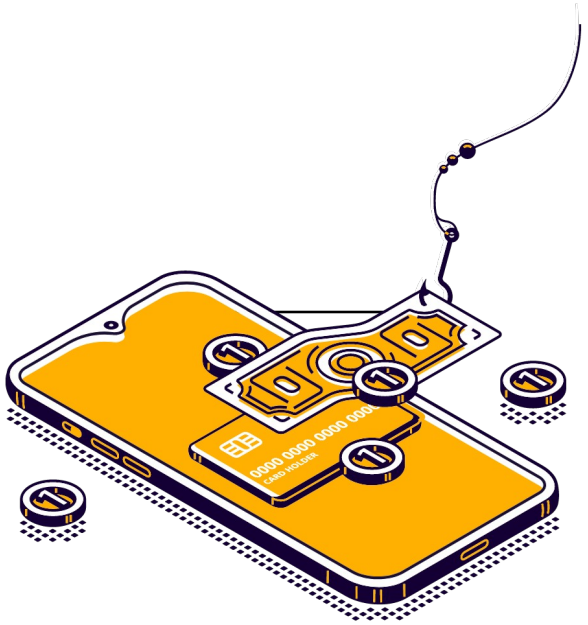
La parola **Smishing** indica una truffa di phishing realizzata con l'invio di SMS all'interno dei quali è presente un link da cliccare che rimanda a landing page in cui sono presenti moduli o form da compilare.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Vishing

La parola **Vishing** indica una truffa di phishing realizzata attraverso una telefonata reale da parte di un (finto) call center.

La chiamata può essere realizzata attraverso un disco registrato oppure da una persona reale che si finge un operatore che chiede di inserire/dettare, ad esempio, il numero della carta di credito per procedere al pagamento dell'utenza non andato a buon fine precedentemente.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Wi-Fi Hacking

Il **Wi-Fi Hacking** è una truffa che consiste nel generare una falsa rete Wi-Fi aperta (senza password).

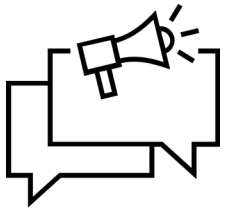
Grazie ad un modem portatile, l'hacker si posiziona in prossimità di un luogo/un'attività che non è fornito di Wi-Fi (esempio, un bar) e ne crea aperta e gratuita col nome dell'attività suddetta e aspetta che i clienti del bar si connettano.

Durante la connessione i dati vengono registrati e rubati.

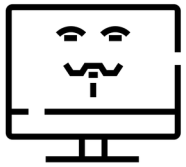
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Gli Strumenti dell'Hacker: Tipi di Malware

- **AdWare**: strumento che permette di far visualizzare all'utente pubblicità indesiderata



- **Ransomware:** strumento che congela il PC per una successiva richiesta di riscatto



- **SpyWare**: strumento che spia l'utente a sua insaputa

- **Rootkit**: strumento che permette l'accesso da remoto al pc dell'utente vittima

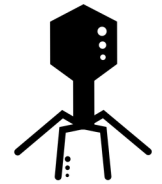
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Gli Strumenti dell'Hacker: Tipi di Malware

- **Worm**: programma in grado di replicarsi autonomamente sfruttando le reti e le falle di sistema per il furto di dati o la cancellazione di file

- **Trojan Horse:** strumento spesso nascosto dagli hacker in file allegato a e-mail di phishing (esempio, file Word) che, una volta scaricati e aperti, installano sul pc un malware

- **Virus**: esattamente come quelli reali, può copiarsi, unirsi ad altri programmi e diffondersi in altri computer



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Consigli di sicurezza per evitare le Truffe Online

Cosa controllare prima di procedere con la navigazione:

- La **connessione Wi-Fi**: se non siamo connessi al nostro Wi-Fi personale, evitare di agganciarci a reti “aperte” che potrebbero essere Wi-Fi Hacking; utilizzare una connessione dati.

- **L’URL** dei siti web: la presenza dell’acronimo **HTTPS** prima del dominio indica un maggior livello di sicurezza.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

Consigli di sicurezza per evitare le Truffe Online

Cosa controllare prima di procedere con la navigazione:

- **Link all'interno di e-mail e SMS**: non cliccarli ma controllare sui siti ufficiali ed accedere da lì in caso fosse necessario

- **Testo:** qualsiasi inesattezza grammaticale, di punteggiatura o di formattazione possono essere indizi di una truffa.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Consigli di sicurezza per evitare le Truffe Online

Cosa controllare prima di procedere con la navigazione:

- **Numeri SPAM e sconosciuti**: non rispondere a numeri che non conosciamo, attivare il blocco spam sullo smartphone per vedere i numeri già segnalati; non richiamare numeri da cui abbiamo ricevuto una chiamata di un solo squillo.

- **Invio di dati sensibili e privati:** dati anagrafici, indirizzi, numeri di carte di credito e conti bancari, anche se si tratta di destinatari conosciuti

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Consigli di sicurezza per evitare le Truffe Online

Cosa controllare prima di procedere con la navigazione:

- **Autenticazione a 2 Fattori**: attivare l'accesso a doppio passaggio ci permette di essere notificati qualora ci sia un tentativo di accesso da parte di un hacker

- **Password sicura:** assicuriamoci di avere delle password differenti per ogni account che abbiamo, studiamole affinché siano sicure ed efficaci e cambiamole periodicamente (ogni 6 mesi circa)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Consigli di sicurezza per evitare le Truffe Online

Cosa controllare prima di procedere con la navigazione:

- **AntiVirus**: rimaniamo sempre protetti su ogni device utilizzando antivirus sicuri e aggiornati

- **Aggiornamenti dei sistemi e delle patch di sicurezza:** di ogni device che utilizziamo; verifichiamo periodicamente se ci sono aggiornamenti non notificati

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Glossario - Definizioni Treccani

- **Antivirus**: Software impiegato per prevenire, rilevare ed eliminare virus informatici, worm, trojan, dialer, spyware e malware
- **Firewall**: Dispositivo hardware o applicazione software che controlla la separazione tra una rete locale e la rete Internet, mediante [...] il quale è possibile implementare un insieme di regole di sicurezza
- **Home Banking**: Servizio bancario che consente all'utente di effettuare direttamente da casa operazioni relative al proprio conto bancario (per es. controllo sui movimenti, pagamento di utenze, richiesta di assegni, bonifici) grazie a un collegamento telematico.
- **HTTPS**: Sigla di Hyper text transfer protocol secure, protocollo in cui la comunicazione tra server e client avviene all'interno di un canale sicuro [...] una certification authority nota, di cui possiede una lista

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Glossario - Definizioni Treccani

- **Privacy & Cookie Policy**: consenso al trattamento dei dati personali e sensibili secondo normativa GDPR - Regolamento 2016/679.
  Trattamento dei tracciamenti delle azioni che un utente effettua su un sito/una piattaforma e relativa sezione di gestione ed impostazione.

- **Phishing**: frode informatica finalizzata all'ottenimento di dati personali sensibili (password, numero di carta di credito ecc.) e perpetrata attraverso l'invio di un messaggio di posta elettronica a nome di istituti di credito, finanziarie, agenzie assicurative, in cui si invita l'utente, generalmente al fine di derubarlo, a comunicare tali informazioni riservate.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Glossario - Definizioni Treccani

- **Account**: registrazione presso un provider di un utente che voglia accedere a un determinato servizio e, per estensione, l'insieme delle informazioni (nome, password, ecc.), depositate presso il provider medesimo, che identificano l'utente.

- **Password**: parola di riconoscimento impiegata a scopo di sicurezza per garantire che l'uso di una risorsa sia concesso solo agli utenti autorizzati

- **Pop Up:** Finestra del web browser che si apre per presentare informazioni aggiuntive, approfondimenti, un altro sito Internet o, più frequentemente, annunci pubblicitari.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Glossario - Definizioni Treccani

- **Wallet**: portafoglio digitale
- **Banner:** titolo o logo che si colloca, per lo più a scopi pubblicitari, nei documenti elettronici, e in particolare nelle pagine web, composto generalmente a colori e con caratteri particolarmente ricchi ed elaborati. Inserito in una pagina di un sito web ha lo scopo di attrarre traffico verso un altro sito attraverso un collegamento diretto.
- **E-Commerce**: Transazione e scambio di beni e servizi effettuati mediante l'impiego della tecnologia delle telecomunicazioni e dell'informatica (Internet, Intranet, personal computer, televisione digitale ecc.). Le [...] Business, fra imprese); B2C (Business to Consumer, fra imprese e consumatori); C2C (Consumer to Consumer, fra consumatori).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

TRUST aWARE

Enhancing Digital Security, Privacy and TRUST in softWARE

Grazie per l’attenzione.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377