CERTFin

CERT Finanziario Italiano

LA TUTELA DELLA FIDUCIA

Garantire la sicurezza nei pagamenti evoluti

Romano Stasi

Direttore Operativo

CERTFin

IL SALONE DEI PAGAMENTI PAYVOLUTION

TLP GREEN

Il CERTFin

A gennaio 2017 nasce il CERTFin, un **percorso di cooperazione sulla cybersecurity**.

Che cos'è il CERTFin?

Il CERTFin – CERT Finanziario Italiano è un'**iniziativa cooperativa pubblico-privata** finalizzata a innalzare la capacità di gestione dei rischi cyber degli operatori bancari e finanziari e la cyber resilience del sistema finanziario italiano.

Chi può partecipare?

La **partecipazione** al CERTFin è **aperta, su base volontaria, a tutti gli operatori del settore finanziario nazionale**, come: prestatori di servizi di pagamento, intermediari bancari e finanziari, imprese di assicurazione, gestori di infrastrutture di mercato, centri servizi e provider di servizi tecnologici rilevanti per il settore.

Perché un CERT Finanziario?

Il CERT Finanziario Italiano:

- risponde all'esigenza di **innalzare** la **capacità** del settore di **gestione dei rischi cyber** e di **coordinamento** in caso di attacchi;
- è un'opportunità di **coordinamento** centrale delle attività di contrasto e prevenzione per una strategia di cybersecurity di settore sempre più efficace.

DIFFONDERE LE COMPETENZE E FARE AWARENESS

- **Approfondire** temi di **sicurezza informatica** e **normative di riferimento**
- Sviluppare **campagne di sensibilizzazione** sulla cybersecurity
- Svolgere **esercitazioni** e **simulazioni su scenari cyber**

SVILUPPARE ULTERIORMENTE UNA LOGICA DI ISAC ITALIANO

- **Incrementare l'infosharing** su minacce/ vulnerabilità/ incidenti
- **Svolgere analisi evolutive delle minacce cyber**
- **Studiare il dimensionamento** e l'evoluzione dei fenomeni

COORDINARE LE EMERGENZE E GLI INCIDENTI INFORMATICI

- **Svolgere attività di coordinamento** centrale in caso di **incidente**
- **Supportare operativamente** le strutture di presidio delle **singole realtà**
- **Definire e aggiornare** a livello di settore lessons learned e strategie di risposta

Il CERTFin - che cosa facciamo?

FILONI OPERATIVI

FINANCIAL INFO SHARING AND ANALYSIS CENTER (FinISAC)

Scambio sistematico di informazioni su **minacce/ vulnerabilità/ incidenti**, **aggiornamento** rispetto allo **stato** e all'**evoluzione** della **minaccia cyber** e delle possibili contromisure da prevedere (tecniche e metodiche di attacco, tecnologie di protezione, etc.), report periodici di aggiornamento, **dimensionamento** delle **frodi informatiche** di settore attraverso survey e analisi statistiche.

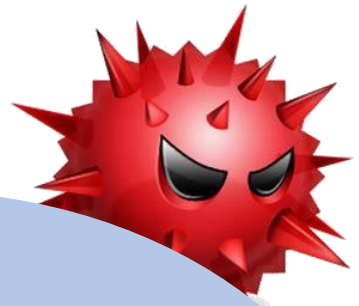
CYBER KNOWLEDGE AND SECURITY AWARENESS

Approfondimenti sulle **normative di riferimento** in materia di **sicurezza e rischio informatico**, definizione di **campagne di sensibilizzazione** sulle tematiche di cyber security, partecipazione a **esercitazioni** e **simulazioni** tra i principali attori del settore bancario e delle entità coinvolte (istituzioni locali, enti internazionali, etc.)

CENTRALE OPERATIVA DI GESTIONE DELLE EMERGENZE CYBER

Analisi e **coordinamento** in caso di **incidente/artefatto/ vulnerabilità di sicurezza**, in **affiancamento** alle **capacità interne** del soggetto Aderente di natura tecnologica e/o di processo, **aggiornamento** e **condivisione** a livello di settore delle strategie di risposta più appropriate, maturate sulla base delle lessons learned apprese dagli altri Aderenti

Gli ultimi fenomeni rilevati



Frodi informatiche

- Campagne CEO Fraud
- Frodi tramite PEC
- Phishing
- SIM Swap

Attacchi a dati e informazioni

- Compromissione account – Ursnif
- Campagne malware (false fatture, etc.)
- Campagna malspam falso mittente Banca d'Italia

Attacchi alla disponibilità di servizi/asset IT

- Attacchi DDoS
- Minacce Ransom DDoS
- Scansioni malevole

Gli Italiani e la cyber security

- **diffusa preoccupazione** per la sicurezza delle transazioni on line (solo il 19% in EU dichiara di non essere preoccupato) ,
- maggiori preoccupazioni sulla **sicurezza dei pagamenti online** (43%, +6% vs 2014) e sull'**abuso di dati personali** (43%, +5% vs 2014),
- il 32% degli intervistati afferma di preferire operazioni bancarie o l'acquisto di beni o servizi di persona (media EU: 27% - l'Italia è tra i paesi con il tasso più elevato).

La sicurezza informatica non è reputata una sfida molto importante dagli Italiani (45% intervistati vs 56% media EU. Tra i Paesi con il tasso più basso, seppure in crescita: +15% vs 2014).

Non emergono rilevanti differenze socio-demografiche, seppure la fascia più adulta sia più preoccupata per le transazioni on line, mentre i giovani ritengano più possibile non ricevere i prodotti ordinati on line. Ciò dipende verosimilmente dal tipo di attività svolta più di frequente sul web.

Fonte: Survey conducted by TNS opinion & political at the request of the European Commission, Directorate-General for Migration and Home Affairs: Field June 2017, Report September 2017.

Come ci proteggiamo?

→ Come ci proteggiamo? … Ma siamo sicuri che ci proteggiamo?

A fronte della nostra preoccupazione in tema di cyber security, attuiamo alcuni **comportamenti virtuosi** ma ancora **in misura ridotta rispetto alla media EU**:

- **cambio della password negli ultimi 12 mesi:**
  - email (37% vs 41% EU)
  - social network (23% vs 29% EU)
  - on line banking (20% vs 29% EU)
  - shopping website (7% vs 17% EU)
- **apertura email solo da indirizzi noti** (28% vs 35% EU),
- **accesso a Internet solo dal proprio computer** (27% vs 36% EU),
- **installazione o aggiornamento dell'antivirus** (26% vs 45% EU),
- **minore diffusione informazioni personali on line** (23% vs 39% EU),
- **uso password diverse per siti diversi** (17% vs 28% EU).

N.B. in alcuni casi il cambio di password può essere indotto dal sito/network e non essere un'azione spontanea di tutela dell'utente.

Pochi hanno preso l'iniziativa di ridurre i beni e i servizi che acquistano on line (11% vs 12% EU) o ridotto il banking on line (9% vs 10% EU).

Fonte: Survey conducted by TNS opinion & political at the request of the European Commission, Directorate-General for Migration and Home Affairs: Field June 2017, Report September 2017.

Quindi…

Gli Italiani:

- risultano ancora **poco sensibili al tema della cyber security** ma, parallelamente alla sempre maggiore digitalizzazione, **stanno acquisendo consapevolezza** della presenza di rischi legati alle transazioni online,
- nutrono particolare preoccupazione in relazione alla sicurezza dei pagamenti on line,
- malgrado la preoccupazione, pochi abbandonano i servizi/pagamenti on line o preferiscono quelle di persona, segnale di un **trend di digitalizzazione in crescita** e dell'esigenza di **sensibilizzare/ educare in materia**.

AWARENESS,

SENSIBILIZZAZIONE,

COMUNICAZIONE,

EDUCAZIONE.

Le iniziative di awareness in Europa

Dal 17 al 23 ottobre (ECSM), le forze dell'ordine di tutti i 28 Stati membri dell'UE, 5 Stati non membri, 24 associazioni bancarie nazionali e realtà attive contro i cibercriminali si sono unite per aumentare l'awareness sul fenomeno criminale delle **CYBER SCAMS**, attraverso una campagna di comunicazione sui social media e sui siti di polizie, associazioni bancarie e istituzioni finanziarie.

- Phishing/Vishing/Smishing
- Spoof/ Fake Websites/ Website Spoofing
- Data stealers via social media
- On line shopping e investment scams (fake trader scams)
- CEO Fraud/BEC (business e-mail compromise)
- Invoice Fraud (invoice redirection)
- Romance scams

Il CERTFin è stato partner per l'Italia della campagna di awareness Europol/ EBF dedicata alle più comuni truffe on line.

Campagna Cyber Scams - focus

Post coordinati con gli account dei promotori (Europol ed EBF) sono stati pubblicati sui maggiori **social network**, utilizzando come richiamo i **banner** creati ad hoc e alcune immagini fortemente esplicative.

Sul sito **CERTFin.it** sono state create pagine web dedicate alle diverse tipologie di truffe on line.

Ogni tipologia di truffa viene spiegata indicando:

- **descrizione** del meccanismo criminale,
- **segnali** da non sottovalutare,
- **consigli** su che cosa fare per proteggersi come privato / dipendente / azienda.

Inoltre, le informazioni sono riportate anche in un'**infografica** per favorirne la fruizione e circolazione.

Attraverso il CERTFin, la campagna è stata ripresa da **10** banche italiane, che ne hanno reso disponibili i contenuti alla propria clientela e/o ai propri dipendenti.

Campagna di awareness CERTFin

Il CERTFin, parallelamente alla sua attività istituzionale, sta realizzando una **campagna di sensibilizzazione** sui rischi connessi all'utilizzo dei sistemi di pagamento digitali e sulle buone pratiche da adottare per evitare di incorrervi.

La campagna:

- si rivolgerà all'**ampio pubblico** dei detentori di conti corrente on line/ sistemi di pagamento digitali,
- si **affiancherà alle attività già realizzate in materia dai singoli istituti** di credito per essere ripresa nei loro canali di comunicazione.

OCCHIOALCLIC

Le mille opportunità e attività che Internet offre comunicate attraverso l'immagine di un computer aperto da cui esplode un mondo coinvolgente di colori e positività: la ricchezza di Internet che affascina ormai tutti.

MA.

Così come il mondo reale che ci circonda, anche il mondo virtuale non è esente da qualche insidia, se non si presta attenzione. **Occhioalclic** è la risposta e l'invito ad adottare un atteggiamento virtuoso di buone pratiche nelle operazioni on line.

TRE PAROLE PER:

- catturare l'attenzione dell'utente,
- stuzzicare la sua curiosità,
- sensibilizzarlo a far restare Internet un luogo meraviglioso grazie al suo operato.

OCCHIOalCLIC richiama:

- **vicinanza e semplicità** grazie alla colloquialità usata,
- **memorabilità** e facilità di adozione e ritenzione da parte dei destinatari,
- **call to action:** un invito ad agire, a fare qualcosa,
- il dominio su **cui portare il target** e divulgare i consigli e le attività inerenti la campagna.

Inoltre è "**campagnabile**" in quanto declinabile su più media e può essere esteso a tutto l'universo delle operazioni on line: non solo pagamenti, ma anche **protezione dei dati personali**.

Il piano media

Il target ampio di utenti richiede di uscire da logiche di pianificazione media tradizionali di copertura e frequenza efficaci.

Abbiamo concepito la seguente **STRATEGIA MEDIA**:

- concentrare la campagna in un periodo dato e ristretto, creando un "momentum" comunicativo a dicembre, quando l'attenzione sulle transazioni on line è massima in vista del Natale.
- realizzare strumenti di comunicazione e occasioni per una ripresa e diffusione del messaggio a livello di ufficio stampa/media coverage e facendo leva al contempo sulla rete delle banche del CERTFin.

MEDIA/TOUCHPOINT selezionati:

- Stampa Quotidiana nazionale
- Minisito
- Web Google Display
- Web Posting Facebook
- Video virale e seeding
- Video Infografica
- Leafleting

Work in progress

Ci stiamo concentrando ora sulla realizzazione del **sito occhioalclic.it** e della **campagna su stampa**.

Siamo inoltre alla ricerca dell'idea giusta da produrre per un **video destinato ai social network**.

OCCHIOALCLIC.IT

Il sito **certfin.it** ospiterà la sezione **occhioalclic**, che sarà landing page di tutto il materiale della campagna.
L'area è pensata per ospitare tutte le iniziative di awareness del CERTFin e dei membri del CERTFin di rilievo per il visitatore.

VIDEO VIRALE

Siamo alla ricerca dell'idea che garantisca il successo del video e che aumenti la consapevolezza del destinatario, attivando al contempo comportamenti virtuosi.

In conclusione…

Seguendo le raccomandazioni IOCTA 2018, la difesa più efficace contro i cyber criminali è l'**educazione delle potenziali vittime**

- e tutti noi, quando siamo on line, siamo potenziali vittime.

Incrementare l'awareness, supportare le persone nell'identificazione delle tecniche ingannevoli fa sì che sia gli utenti, sia le loro finanze siano al sicuro on line.

Grazie!