The Innovation Group
Innovating business and organizations through ICT

CERTFin
CERT Finanziario Italiano

Sicurezza e frodi informatiche in banca: il ruolo del CERTFin

Milano, 31 maggio 2018

Romano Stasi

*Direttore Operativo **CERTFin***

*Segretario Generale **ABI Lab***

TLP GREEN

Agenda

- LO SCENARIO 2017 SU SICUREZZA E FRODI INFORMATICHE NELLE BANCHE ITALIANE
- IL CERTFIN A SUPPORTO DELLA RESILIENZA DEL SISTEMA FINANZIARIO NAZIONALE

Il rischio cyber nell'era digitale

Il **2017** è stato segnato da casi più o meno eclatanti di attacchi **cyber** che hanno avuto una forte **risonanza mediatica**

Alcuni esempi:

Oltre alle **potenziali perdite** economiche, i livelli di rischio **reputazionale** associati alle **minacce cyber** hanno assunto una **rilevanza** talmente elevata da richiedere un'**azione strategica** e **coordinata** in grado di agire su più dimensioni, da quella orizzontale cross-industry a quella verticale socio-politica, per prevenire e contrastare **attacchi** e **frodi**

Avere un **quadro d'insieme** degli **attacchi** e delle **frodi informatiche** permette di disegnare un **«cyber threat landscape»** di settore, in grado di supportare la **definizione** delle **contromisure** più opportune

Sicurezza e frodi informatiche in banca
Rilevazione 2017

CERTFin
CERT Finanziario Italiano

- **29 organizzazioni** rispondenti, tra banche, gruppi e outsourcer, rappresentativi del **75%** del settore in termini di sportelli
- Periodo temporale di analisi: **dal 1° Gennaio al 31 Dicembre 2017**, dati raccolti in maniera distinta per segmento Retail e Corporate
- Tipologie di **transazioni** online prese in esame: **Bonifico** (Italia, Estero), **Ricarica carta prepagata** e **Ricarica telefonica**. Sono **escluse** le **transazioni online tramite carta**.

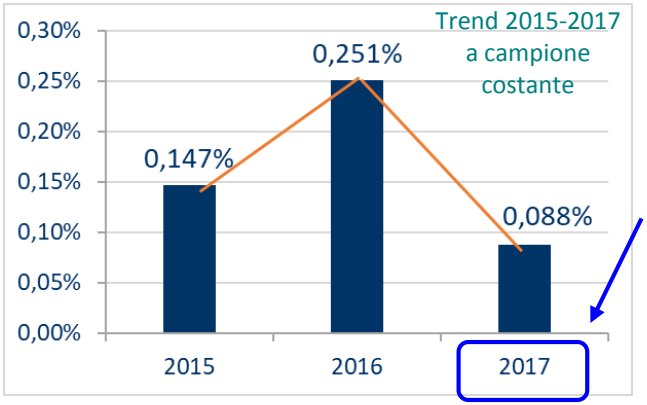
Furto di credenziali digitali e danno economico
Clientela Retail e Corporate

CERTFin
CERT Finanziario Italiano

Clientela Retail: l'**81,5%** dei rispondenti ha registrato nel **2017** un **furto di credenziali di accesso** ai servizi di Internet / Mobile Banking

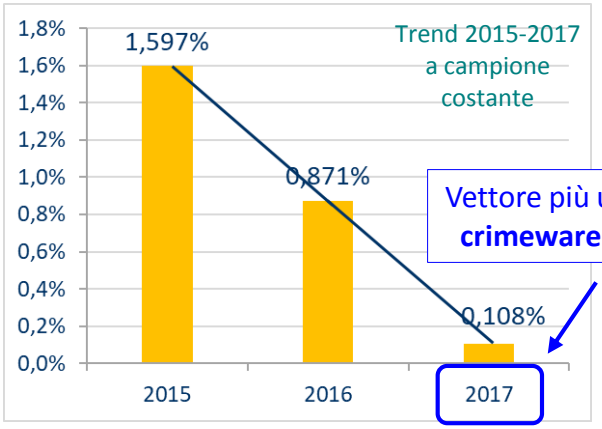
Clientela Corporate: l'**84,6%** dei rispondenti ha registrato nel **2017** un **furto di credenziali di accesso** ai servizi di Internet / Mobile Banking

% di clienti attivi che ha subito un furto di credenziali



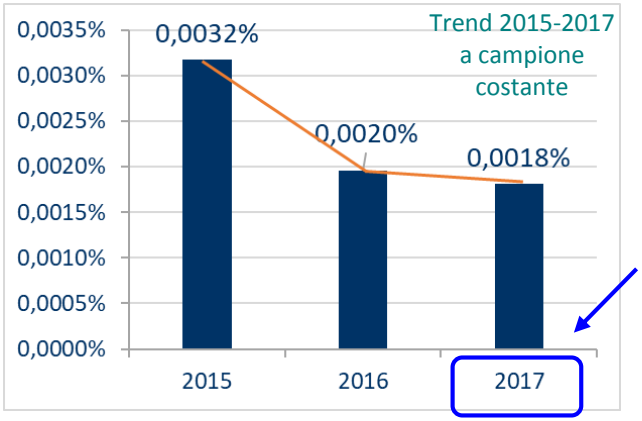
Phishing principale vettore di furto di identità (**91,1%**)

% di clienti attivi che ha subito un furto di credenziali



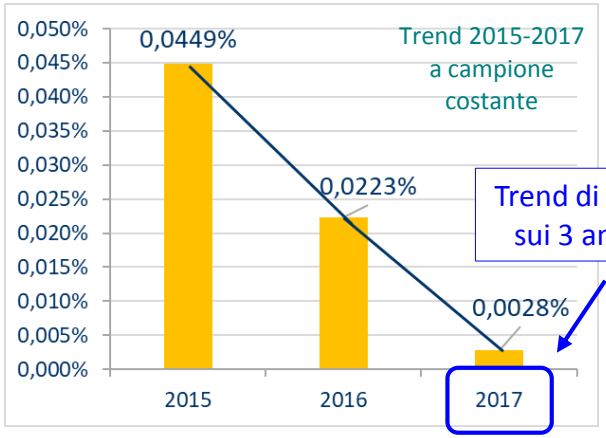
Vettore più utilizzato: **crimeware (71,8%)**

% di clienti attivi che ha perso denaro



Solo **1 ogni 55.500** utenti attivi ha subito un danno economico

% di clienti attivi che ha perso denaro

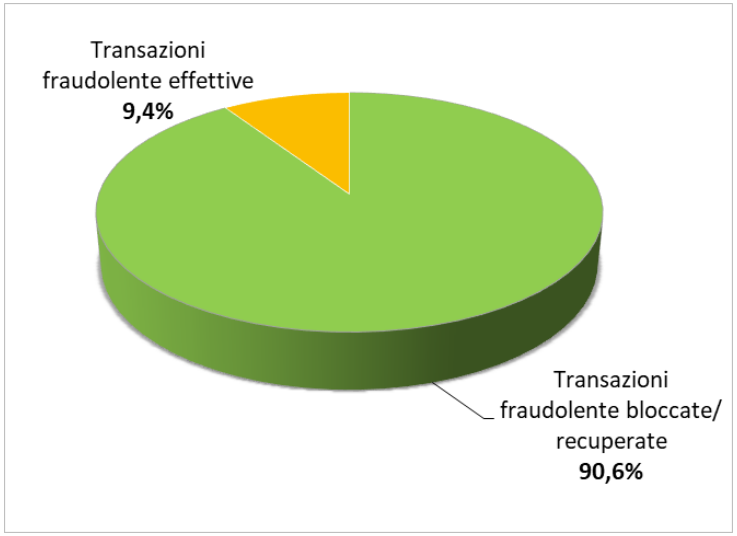


Trend di decrescita sui 3 anni: **-94%**

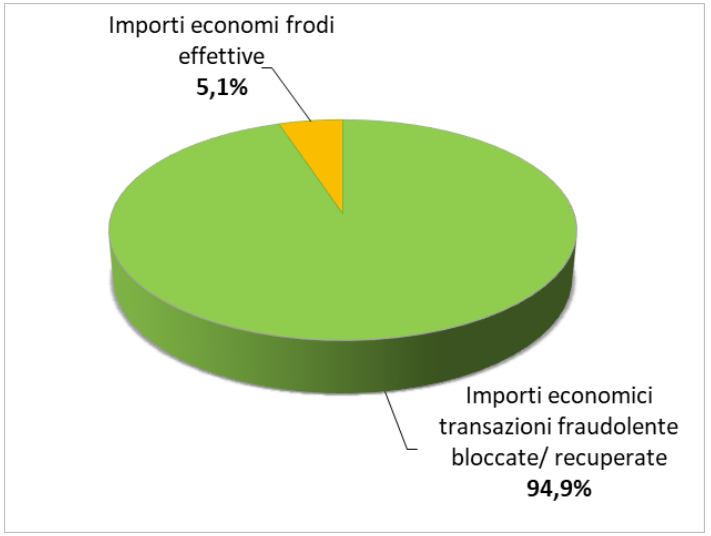
Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Information Security e Frodi Internet e Mobile Banking, 2018 (Campione complessivo: 29 rispondenti)

Scenario complessivo transazioni anomale
Analisi su tutta la clientela

Ripartizione percentuale delle tipologie di transazioni **anomale (bloccate, recuperate ed effettive) – Numero di accadimenti** (complessivo Retail e Corporate)



Ripartizione percentuale delle tipologie di transazioni **anomale (bloccate, recuperate ed effettive) – Importi economici** transati (complessivo Retail e Corporate)



→ La rilevazione di attacchi e frodi e le conseguenti azioni di blocco sono sempre più **tempestive**, grazie anche alle **soluzioni tecnologiche** presenti in banca, come i tool di **analisi automatica dei log di accesso (92,6%)** e gli **strumenti di monitoraggio delle transazioni** anomale (**88,9%**)

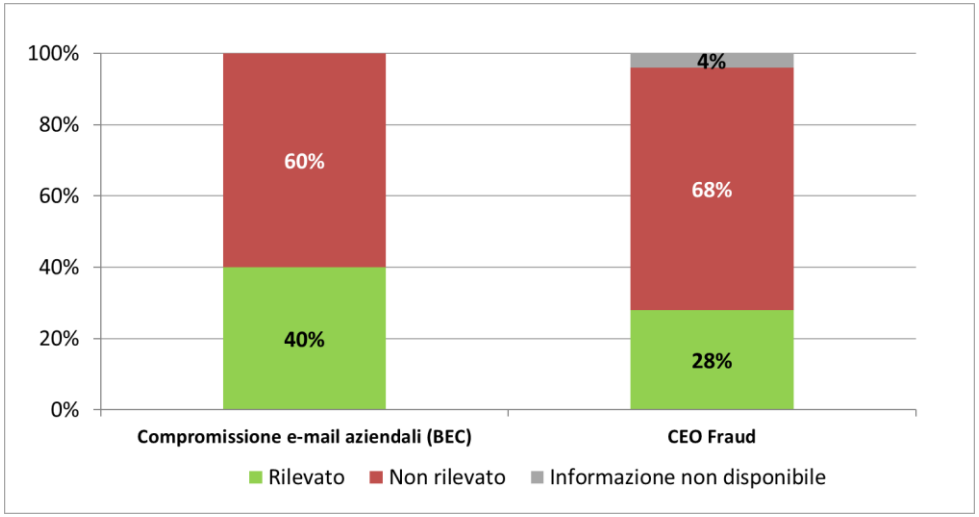
A conferma della costante attenzione ai temi legati al contrasto del crimine informatico, il **26,5%** del **budget sicurezza IT** è dedicato alla **prevenzione/contrasto delle frodi**

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Information Security e Frodi Internet e Mobile Banking, 2018 (Campione complessivo: 29 rispondenti)

CEO Fraud e BEC: le nuove frontiere del social engineering

CERTFin
CERT Finanziario Italiano

Rilevazione di frodi basati su tecniche di social engineering



Si sta assistendo ad un **incremento delle campagne** di **CEO Fraud** e **BEC** a livello sia internazionale che italiano

BEC: 171 tentativi di frode rilevati, di cui circa il **36%** è andato a buon fine

CEO: 36 tentativi di frode rilevati, di cui circa il **6%** è andato a buon fine. Il **volume** di **perdite economiche** associate al fenomeno del **CEO Fraud** è circa **doppio** rispetto alle perdite associate ai casi di **BEC**.

Accanto al continuo aggiornamento delle misure di controllo è fondamentale l'**attività di sensibilizzazione mirate alle aziende clienti sui rischi del social engineering**, in particolare verso dipendenti con delega all'operatività on line

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Information Security e Frodi Internet e Mobile Banking, 2018 (Campione complessivo: 29 rispondenti)

In sintesi…

In continuità con quanto rilevato negli anni precedenti, anche per il **2017** le banche italiane hanno introdotto **misure tecnologiche** e di **processo** che hanno **consentito** di **contenere efficacemente** gli **attacchi** finalizzati alla sottrazione di **denaro** dai conti della clientela…

…ma è opportuno rivolgere **crescente attenzione** ai **nuovi modelli di attacco** usati dai frodatori che, nell'ecosistema digitale dai confini più estesi, si stanno concentrando in misura particolare sulle **vulnerabilità umane** o su **processi** che vedono il **coinvolgimento** di **altri operatori,** anche **esterni** alla banca

Accanto alle **azioni** intraprese dai **singoli** operatori, una continua attività di **sensibilizzazione** delle **persone e una collaborazione operativa** tra banche e con stakeholder esterni diventano elementi **chiave** per garantire una **crescente capacità di risposta** e di **prevenzione** ad **attacchi e frodi cyber**

Nella lotta al crimine informatico, la condivisione delle esperienze diventa una delle fonti principali di conoscenza

CERTFin - CERT Finanziario Italiano
Overview

CERTFin
CERT Finanziario Italiano

FILONI OPERATIVI

FINANCIAL INFO SHARING AND ANALYSIS CENTER (FinISAC)

CYBER KNOWLEDGE AND SECURITY AWARENESS

CENTRALE OPERATIVA DI GESTIONE DELLE EMERGENZE CYBER

GOVERNANCE E OPERATIVITÀ

- ✓ **Presidenza** condivisa tra **ABI e Banca d'Italia**
- ✓ **Direzione Operativa** in carico al **Consorzio ABI Lab**
- ✓ **Modello campus – Team Virtuale** a supporto della Direzione Operativa
- ✓ **Soggetti esterni esperti** e qualificati a svolgere approfondimenti e analisi

ADESIONI

- **42 soggetti aderenti** al CERTFin
- **9 partecipanti al Team Virtuale**
- **In attesa adesione di altre tipologie di soggetti**

TF-CSIRT Trusted Introducer

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY — AUTHORIZED TO USE CERT

www.certfin.it

info@certfin.it

Il CERT Finanziario Italiano come network di collaborazioni per rafforzare la sicurezza

CERTFin
CERT Finanziario Italiano

CERT di settore / Entità europee di cybersecurity

Nordic CERT

NCSC-UK

…

CERT nazionali di altri Paesi

CERT Austria

CERT Lussemburgo

CERT Polonia

CERT Svizzera…

Istituzioni e centri di competenza

DIS

CERT Nazionale/ CERT-PA

MEF

Università

…

Forze dell'ordine

polizia delle comunicazioni

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

C.N.A.I.P.I.C

Telco Provider

CERTFin

CERT Finanziario Italiano

Organizzazioni internazionali

SWIFT

FINANCIAL SERVICES ISAC

European FI-ISAC

…attraverso ABI Lab

Constituency

COMING SOON!

Banche e operatori finanziari

Team Virtuale

Assicurazioni e altri operatori

Attività di information sharing
Principali fenomeni rilevati e lesson learned (1/2)

CERTFin
CERT Finanziario Italiano

Gennaio 2017 - Eye Pyramid

- Rilevato appena 5 giorni dopo la costituzione del CERTFin
- Il fenomeno ha rappresentato l'occasione per «testare» il punto di partenza in tema di collaborazione operativa e network creato negli anni del Presidio.Internet

Aprile 2017 – Blocco manuale bonifico disconosciuto

- Bloccato un bonifico fraudolento grazie alla collaborazione degli attori coinvolti
- È stato possibile impedire la fase di cash out bloccando la carta associata al mulo, con la cooperazione del CERTFin e la collaborazione della banca destinataria. Necessaria una maggior strutturazione nello scambio tempestivo di informazioni su operazioni fraudolente →

Maggio - Giugno 2017 – Wannacry & Petya/Not Petya

- Elevato impatto mediatico, cross-industry e cross-country
- Si è ritenuta necessaria un'attività di inforsharing coordinata almeno a livello italiano, avviando poco dopo i lavori per la definizione dell'architettura nazionale di information sharing (WIP, per il settore sono presenti il CERTFin ,Intesa Sanpaolo e UniCredit)

Frodi informatiche

Attacchi a dati/ informazioni

Attacchi alla disponibilità di servizi/ asset IT

Attività di information sharing
Principali fenomeni rilevati e lesson learned (2/2)

CERTFin
CERT Finanziario Italiano

Agosto 2017 – Attacco in Ucraina

- Minacce di attacchi in concomitanza con festività nazionali (Independence day) e comunicati stampa della BCN
- Elevato livello di attenzione anche in Italia, primi contatti con il DIS per allineamento sullo stato dell'arte nel settore bancario → Opportunità di rafforzare la relazione

Gennaio 2018 – Attacchi DDoS in Olanda

- Attacco diffuso a diversi soggetti (banche e organizzazioni della PA)
- 4 delle principali banche olandesi sono state attaccate; impatti non gravi (indisponibilità di alcuni servizi per pochi minuti), ma il CERTFin si è subito attivato con il CERT Nazionale e i diversi network → E se succedesse in Italia?

Aprile 2018 – SIM Swap #N

- Nuovi fenomeni di SIM swap, che hanno generato frodi
- Emergono nuovamente le necessità di rafforzare le iniziative di awareness verso la clientela e di cooperazione con i TELCO, anche individuando servizi e strumenti antifrode

Maggio 2018 – Frodi tramite PEC

- Nessun attacco alle banche, ma sfruttate vulnerabilità di processo di altri soggetti
- Importante rafforzare il livello dei controlli a livello di sistema Paese, le organizzazioni criminali sono sempre più attente a sfruttare anche la minima vulnerabilità

Frodi informatiche

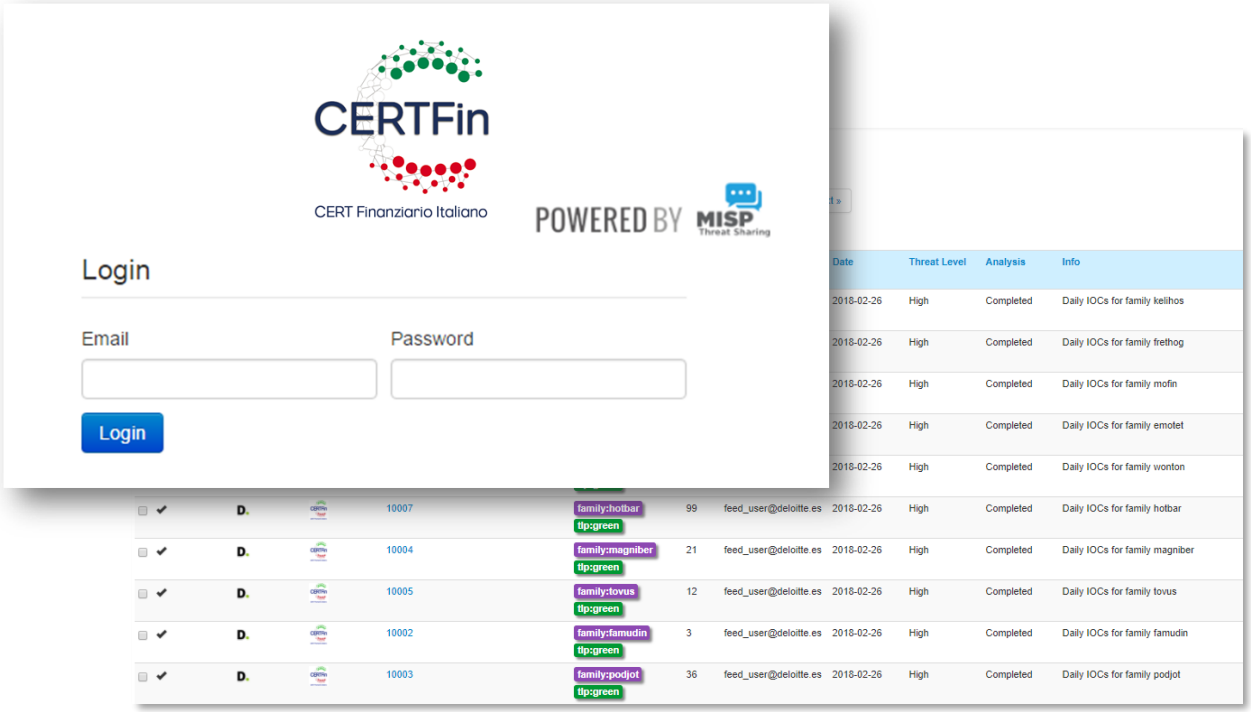
Attacchi a dati/ informazioni

Attacchi alla disponibilità di servizi/ asset IT

Evoluzione attività di information sharing
Abilitazione istanza MISP CERTFin

CERTFin
CERT Finanziario Italiano

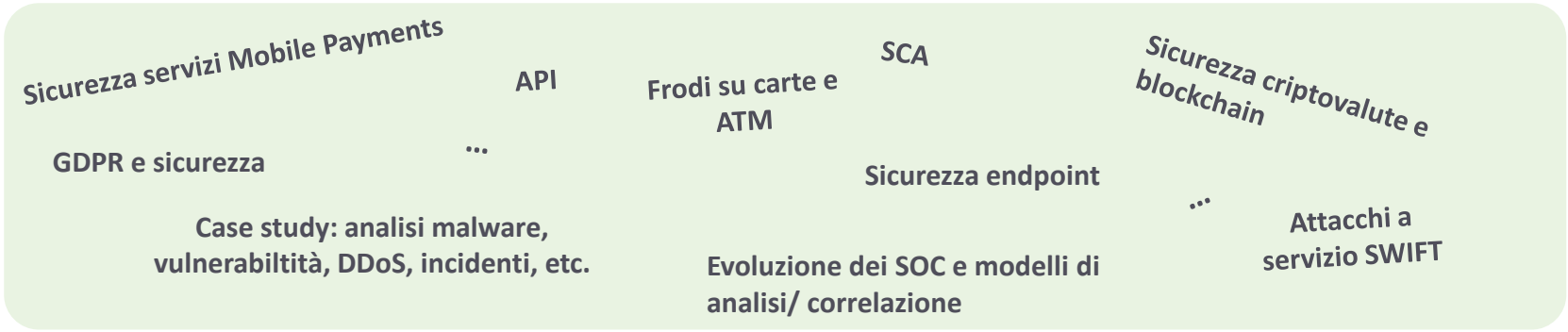
- Con l'obiettivo di innalzare la capacità di cyber resilience della propria constituency, il CERTFin ha avviato l'attività di information sharing sulla piattaforma MISP (Malware Information Sharing Platform - http://www.misp-project.org/index.html)
- L'obiettivo è **incrementare lo scambio costante e tempestivo di informazioni** utili a rilevare, prevenire e contrastare potenziali attacchi che possano mirare l'integrità, la disponibilità e la riservatezza delle informazioni
- La MISP consente agli utilizzatori di ricevere informazioni relative ad attacchi e fenomeni fraudolenti in modo strutturato e in formato "**machine readable**" (STIX)



NB! Per **permettere la tempestiva e immediata condivisione degli IoC** relativi a minacce e attacchi rilevati anche con coloro che non utilizzano la MISP, è stato reso **disponibile** il **feed CERTFin in formato STIX**

Awareness e approfondimenti

- Nel **2018** è stato avviato **un ciclo di webinar, le CERTFin Webinar series**, con sessioni **verticali** dedicate a specifiche tematiche con l'obiettivo di condividere competenze all'interno della constituency



- I webinar:
  - svolti con cadenza circa **bimestrale**, offrono ai membri della constituency la possibilità di **condividere analisi e studi svolti** su specifici ambiti di interesse
  - sono curati direttamente dalla Direzione Operativa, che assicurerà il mantenimento di un **profilo tecnico** dei diversi seminari, coinvolgendo **personale esperto**
  - sono **riservati alla constituency** del CERTFin

Il CERTFin avvierà nel corso del 2018 una nuova **campagna di sensibilizzazione** sui temi legati alla cyber security, per favorire l'adozione di **comportamenti virtuosi** nell'utilizzo dei sistemi bancari online