Sensibilizzare le persone, riconoscere gli attacchi per evitare di cadere vittime del cyber crime

Milan, 10 March 2020

Contenuti

Sfide e Minacce 1/4

SFIDE

- Cyber & Data Breaches
- Faster Payments
- Evolving Digital Channel
- Open Banking (PSD2)

MINACCE


Il Messaggero.it

«Sim-swap», banda di campani ruba 9.000 euro dal conto online: ecco come ha fatto


QuiFinanza NOTIZIE E MERCATI SOLDI FISCO E TASSE GREEN LAVORO PENSION

Temi Caldi: • Coronavirus • Bonus casa 2020 • Limite contanti • Flat tax 2020

Home > Informazioni utili > Nuova truffa per Unicredit, BNL e Intesa Sanpaolo: attenzione al conto

Nuova truffa per Unicredit, BNL e Intesa Sanpaolo: attenzione al conto

PADOVAOGGI ≡ Sezioni Cronaca

Cronaca / Camposampiero

Dal cellulare accedono al conto in banca: gli hacker spillano 22mila euro a un padovano

Due uomini italiani sono stati denunciati per aver carpito i dati sensibili di un cinquantottenne dell'Alta Padovana accedendo al suo home banking tramite la sim del cellulare


LA STAMPA

topnews

torinosette tuttigusti tuttolibri tuttosalute tuttoscienze tuttosoldi

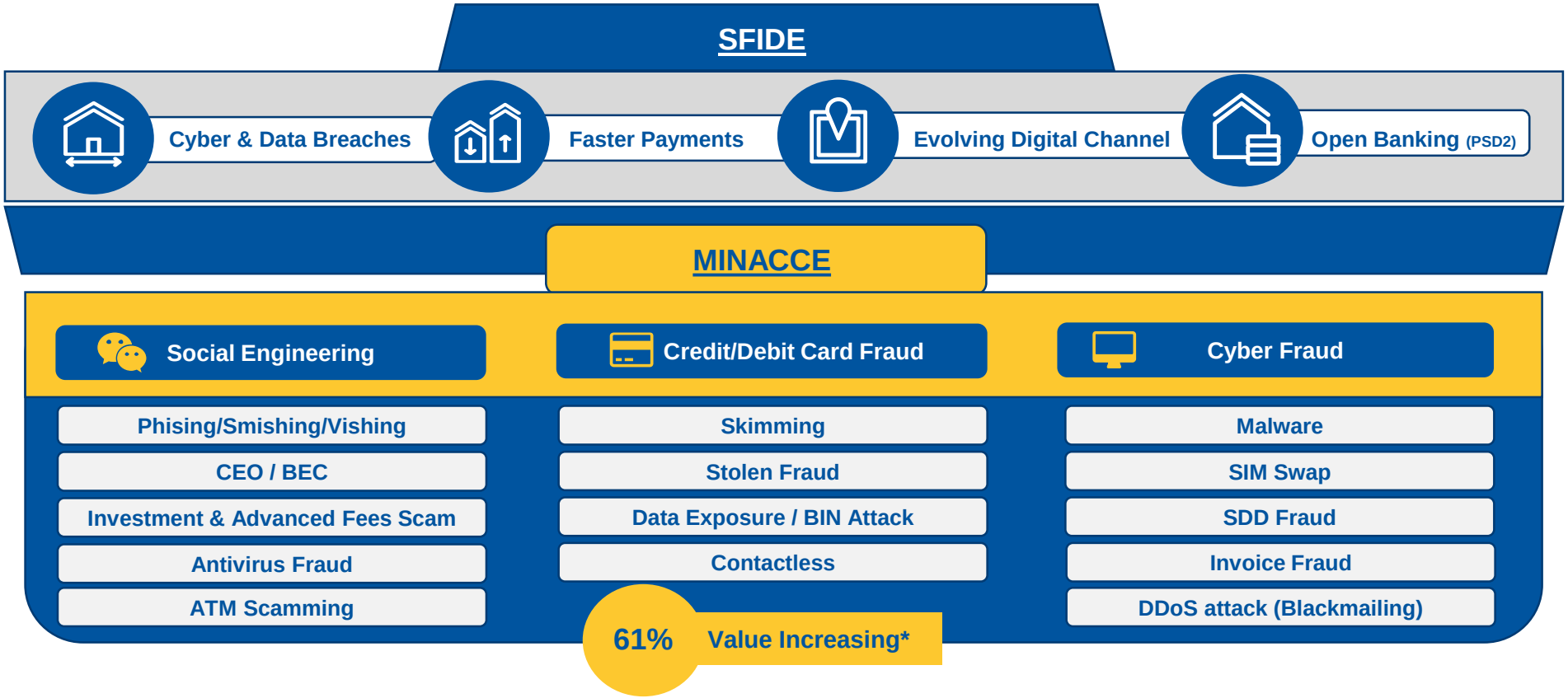
ECONOMIA&FINANZA EDIZIONI LOCALI FIRME LETTERE&IDEE PRIMO PIANO SPORT STAMPA PLUS TEMPI MODERNI

TOP NEWS / ECONOMIA E FINANZA

La Fabbrica delle frodi: ecco che cosa c'è dietro le telefonate che vi invitano a fare investimenti online

Un giro d'affari di 70 milioni di dollari con una rete di call center che promette facili guadagni grazie alle criptovalute. Nella rete molti risparmiatori italiani

Sfide e Minacce 2/4



*Global Banking Fraud Survey 2019 - KPMG

Sfide e Minacce 3/4

SOCIAL ENGINEERING FRAUD

Phising/Smishing/Vishing	Truffa realizzata mediante l'invio di una email/sms contraffatti oppure effettuando una chiamata telefonica apparentemente proveniente dalla Banca, in cui si invita la vittima a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.
CEO / BEC	Compromissione di email aziendali (con diverse possibili tecniche anche, a volte, di natura intrusiva) attraverso le quali i frodatori, fingendosi dipendenti apicali dell'azienda (o CEO della stessa), chiedono di effettuare bonifici su conti da loro controllati.
Investment & Advanced Fees Scam	La vittima viene contattata telefonicamente da false società di trading/brokerage, che propongono di effettuare investimenti su vari prodotti (in particolare, criptovalute) promettendo guadagni elevati a fronte di un rischio contenuto. I frodatori convincono il cliente ad effettuare versamenti a mezzo bonifico (a volte installano prodotti per accedere loro stessi al conto del cliente) su conti correnti a loro intestati, facendogli credere di andare ad alimentare un conto trading, mentre in realtà si appropriano del denaro del cliente.
Antivirus Fraud	Adware che fa comparire, in fase di navigazione internet, una finestra nella quale si comunica che il pc è infettato da un virus e che, per eliminare il virus, è necessario chiamare un numero di telefono. Il cliente chiama quel numero ed i frodatori lo convincono a sottoscrivere un abbonamento (con pagamento mensile) per essere protetto. Molto spesso inoltre i frodatori installano sul computer del cliente un remote access tool tramite il quale effettuano accesso all'home banking ed operazioni fraudolente sullo stesso
ATM Scamming	I frodatori inducono la vittima a ricaricare presso un ATM una carta ricaricabile in loro possesso su falsa promessa di ricevere invece un accredito per acconto di un bene realmente messo in vendita online dalla vittima.

Sfide e Minacce 4/4

CREDIT/DEBIT CARD FRAUD

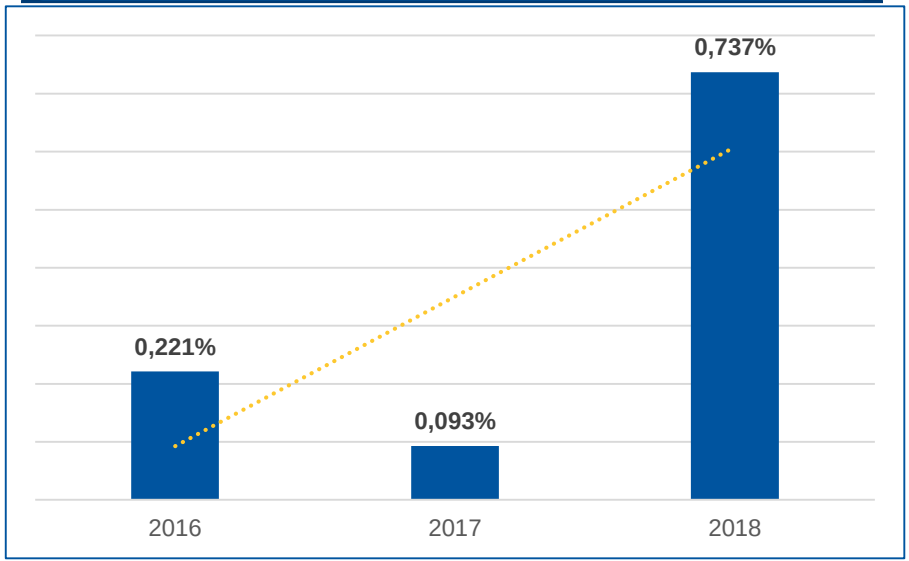
Skimming	Cattura dei dati della carta durante il prelevamento di contanti agli sportelli automatici. I frodatori occultano uno “skimmer”, in grado di catturare i dati presenti nella banda magnetica della carta. Una minuscola telecamera, montata in modo da passare inosservata sullo sportello bancomat, registra l’introduzione del PIN e la trasmette al truffatore. I dati così carpiti verranno successivamente utilizzati in paesi dove è ancora possibile il prelievo del denaro in banda magnetica.
Stolen Fraud	Scenario di frode che mira a clonare ed intercettare i dati sui carta chip con autenticazione PIN. I frodatori carpiscono il PIN tramite dispositivi installati su device usati comunemente (es. Cassa automatica metro). Una volta ottenuto il PIN, il possessore viene seguito per essere derubato della carta.
Data Exposure / BIN Attack	I frodatori ottengono i numeri di carte valide e provano ad acquistare beni e servizi su siti di e-commerce a volte anche fraudolenti.
Contactless	I frodatori tramite un POS si avvicinano alla vittima e sfruttando la funzionalità «contactless» (RFD o NFC) sottraggono cifre basse, sotto il livello di soglia che richiede l’autenticazione, dalla carta della vittima

CYBER FRAUD

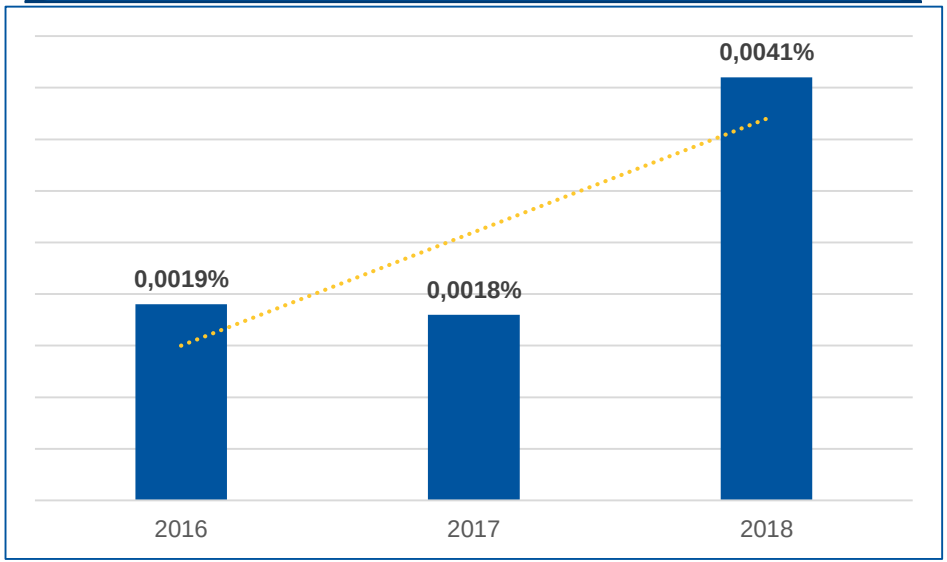
Malware	I codici dell’home banking vengono carpiti tramite virus e/o malware presenti su uno o più dispositivi del cliente (*Man in the Browser*)
SIM SWAP	Sostituzione, da parte dei frodatori, della scheda SIM del cliente con una SIM avente lo stesso numero telefonico e tramite la quale i frodatori stessi sono in grado di confermare operazioni dispositive, avendo accesso agli OTP inviati dalla Banca.
Invoice Fraud	I frodatori compromettono email private e intercettano eventuali fatture che il cliente riceve a mezzo email, sostituendole con fatture del tutto simili in cui cambiano l’iban sul quale effettuare il bonifico.
SDD Fraud	I frodatori aprono un conto aziendale fraudolento ed attivano, solitamente su un ampio numero di clienti di svariate banche, mandati SDD fraudolenti.
DDoS attack (Blackmailing)	L'acronimo sta per Distributed Denial of Service e consiste nel tempestare di richieste un sito, fino a metterlo ko e renderlo irraggiungibile. L’interruzione dell’operazione di denial viene offerta in cambio di denaro.

Trend delle Frodi

% Clienti attivi Retail
che hanno subito un furto di credenziali



% Clienti attivi Retail
che hanno subito perdite economiche



**Fonte: Report «Sicurezza e Frodi informatiche in banca» Maggio 2019 – CERTFin e ABI Lab*

Cosa può fare il cliente – Gestione Account

GESTIONE ACCOUNT

- Proteggi il tuo fattore di autenticazione (mobile)
- Conserva i codici separatamente e non comunicarli a terzi
- Non postare sui social od online i tuoi dati bancari o dettagli delle tue transazioni
- Mantieni aggiornati antivirus/antispam ed i tuoi dispositivi.
- Avvisa sempre la tua Banca nel caso di eventi sospetti, relativamente alla gestione del tuo conto

Avvisare la Banca in caso di anomalie riscontrate di qualsiasi genere

Es: Malfunzionamento telefono – Richiesta insolita da sconosciuti – Mail sospetta – Mancata ricezione OTP via sms

Cosa può fare il cliente – Gestione Social

GESTIONE “SOCIAL”

- Impara a capire come la tua Banca comunica e nota le differenze con ciò che ricevi nelle comunicazioni
- Diffida di richieste, al telefono o via sms, di credenziali di accesso
- Diffida di proposte di facili guadagni che richiedono anticipo di denaro
- L’interruzione della funzionalità del telefono può essere un pericolo: avvisa la banca del problema
- Verifica che la data dell’ultimo accesso corrisponda con gli accessi realmente effettuati

Avvisare la Banca in caso di anomalie riscontrate di qualsiasi genere

Es: Malfunzionamento telefono – Richiesta insolita da sconosciuti – Mail sospetta – Mancata ricezione OTP via sms

Cosa può fare la Banca 1/2

FATTORI CHIAVE PER PROTEGGERSI DALLE FRODI

Collaborazione settoriale ed istituzionale (ABI, CERTFin, Polizia Postale, altre Banche)

Analisi dei dati in real-time per avere tutti gli elementi necessari per la valutazione della transazione

Valutazione delle transazioni secondo un approccio **Risk-based**

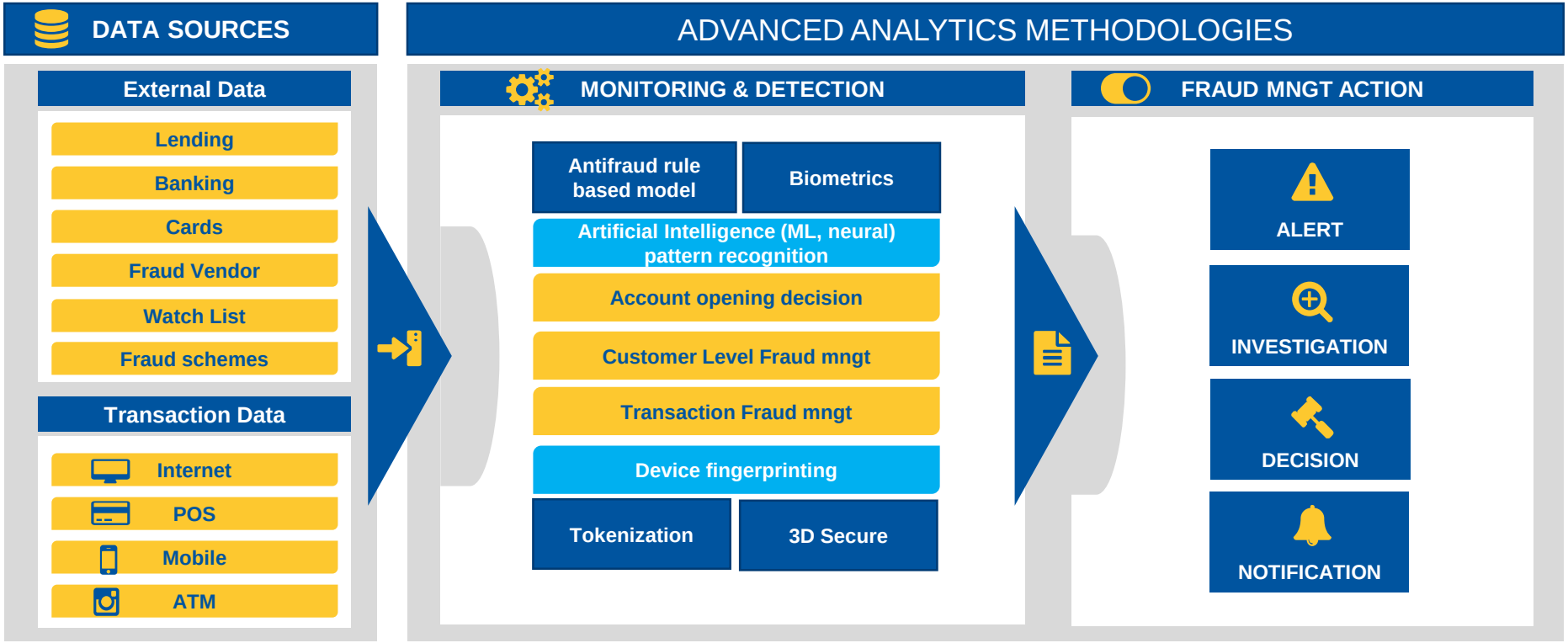
Definizione di un **framework** strutturato di fraud management

Miglioramento continuo dell' approccio di Fraud Risk management utilizzato

Awareness interno e verso i clienti Clienti

Il **fattore umano** continua a ricoprire un **ruolo centrale**: può essere l'anello debole della catena ma anche il più importante strumento di prevenzione.
Pertanto le attività di awareness sia verso il personale interno che verso i clienti della banca risultano essere fondamentali.

Cosa può fare la Banca 2/2



GRAZIE