Panorama

Data 02-11-2006
Pagina 131/32
Foglio 1 / 2

FRODI TELEMATICHE LE INVENZIONI DEI FURBETTI DEL DIGITALE

ATTUALITÀ

Attenti al vishing, truffa via sms

Cellulari, internet e carte di credito sono nel mirino di banditi di nuova generazione. Ma arriva un libro che insegna come difendersi.

■ di GUIDO CASTELLANO

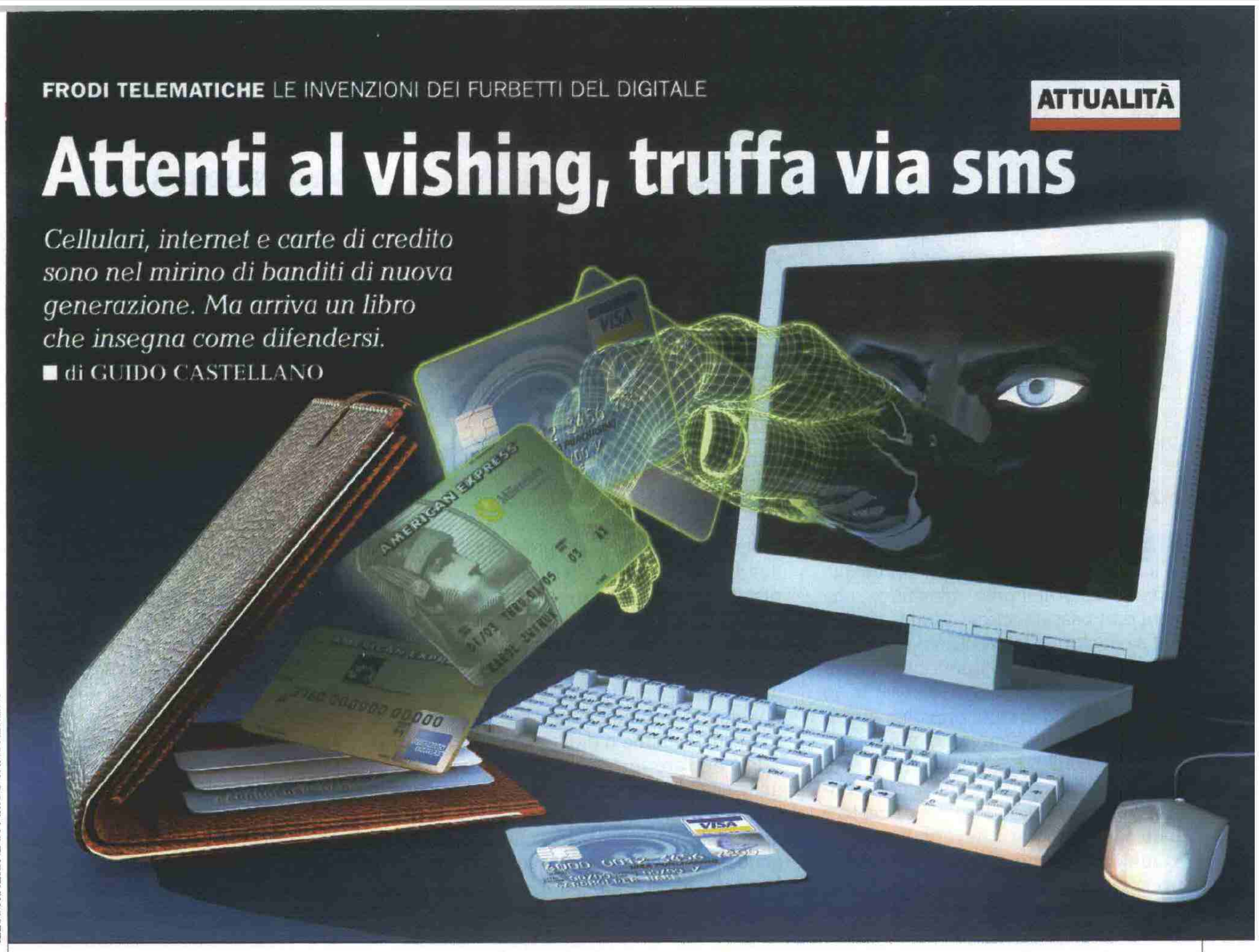


ILLUSTRAZIONE DI MIRCO TANGHERLINI

Squilla il cellulare, è appena arrivato un sms: «Ore 10.45, lunedì 15 ottobre 2006. Effettuata una spesa da 85 euro presso il centro commerciale...». È il rassicurante testo di un nuovo e utile servizio bancario che informa il titolare di una carta di credito o bancomat ogni volta che spende denaro elettronico. Bisogna preoccuparsi, però, se all'ora indicata voi non siete in un ipermercato, ma in ufficio a lavorare.

«È a questo punto che scatta la truffa» spiega il colonnello Umberto Rapetto, comandante del Nucleo speciale frodi telematiche della Guardia di finanza. «Si viene presi dal panico e si cade nella trappola dei cybercriminali. Già perché molti di questi messaggini non vengono mandati dall'istituto di credito, ma dai furbetti del telefonino. Di norma bisognerebbe chiamare la banca e far disattivare la carta» prosegue l'ufficiale «ma spesso si continua nella lettura del messaggio truffaldino che indica in calce un numero da chiamare. Timorose di vedere il conto prosciugato le vittime pigiano il tasto verde del cellulare e chiamano il numero farlocco. Risultato? Risponde una voce elettronica che ha un costo fisso di 15 euro alla risposta. Dopo pochi istanti cade la linea e lo sprovveduto truffato richiama, perdendo in pochi minuti anche centinaia di euro. Oppure risponde un call center» prosegue Rapetto «che chiede di digitare sulla tastiera il numero di carta da bloccare, data di scadenza e il codice di 3 cifre scritto sul retro della plastic card».

Non è ancora stato ben diffuso un utile sistema per evitare la clonazione della carta che già qualcuno ha trovato un modo per guadagnarci a scrocco. Per difendersi da raggiri di questo tipo il colonnello, che oltre a dare la caccia ai cybercriminali insegna in vari atenei, ha scritto il libro *Truffe.com* insieme con la moglie giornalista Maria Teresa Lamberti. Il manuale racconta in dettaglio decine di frodi telematiche, con esempi e «con i suggerimenti per non abboccare e sopravvivere agli imbrogli» spiega la coautrice Lamberti. La truffa sopra raccontata va sotto il nome di «vishing», procedura che inganna con la voce di un rispon- ▶

COPPIA DI SEGUGI
Il colonnello Umberto Rapetto, comandante del Gat, nucleo speciale frodi telematiche della Guardia di finanza, è l'autore, insieme con la moglie giornalista Maria Teresa Lamberti, del libro «Truffe.com» (Cairoeditore, 205 pagine, 13 euro).

Panorama

Data 02-11-2006
Pagina 131/32
Foglio 2 / 2

DE GRANDIS

IN AGGUATO NELL'OMBRA
A sinistra, un lettore di carte bancomat truccato da una gang di romeni. Era in grado di leggere le bande magnetiche e il codice pin che poi inviava, in automatico e con un sms, ai malfattori. In basso, un apparecchio analogo installato all'interno di un normale sistema pos.

ditore automatico e sostituisce con una V (che sta per voice, voce) le prime due lettere dell'ormai noto «phishing», che vuol dire pescare sprovveduti via internet a cui carpire informazioni riservate.

Celati nell'ombra i nuovi cybercriminali vogliono tutti la stessa cosa: le 16 cifre della carta di credito, la data di scadenza e il codice segreto. Oppure i dati del bancomat. Ma quali e quanti sono i nuovi pericoli a cui andiamo incontro? «Ora dilagano i lettori di carte e bancomat taroccati» avverte Lamberti. «Quelli che sono stati modificati con uno skimmer» (dall'inglese skim, che vuol dire leggere velocemente). All'apparenza sembrano normali ma al loro interno hanno un rudimentale ma efficace agente segreto.

«**Quando si inserisce la carta lo skimmer legge i dati della banda magnetica e li memorizza.** Cosa che avviene anche quando si digita il codice» prosegue il colonnello Rapetto. «Poi i dati così illegalmente acquisiti vengono spediti via sms ai malfattori tramite un cellulare nascosto sotto la tastiera del dispositivo contraffatto. Chi riceve l'sms è in grado di preparare una carta assolutamente identica a quella del reale titolare. E di utilizzarla per acquisti illegali. La cosa grave» aggiunge l'ufficiale «è che lo schema elettronico di questi apparecchi è facilmente reperibile in un'infinità di siti web che spiegano come realizzare trucchetti del genere».

Per truffe del genere ci vuole una ben organizzata struttura criminale. Gente in grado di sostituire gli apparecchi che le cassiere usano nei supermercati e di modificare i distributori pos. Ma bisogna stare attenti anche a quei ristoranti che portano al tavolo un lettore di carte senza fili. Sembra una procedura che dovrebbe aumentare la sicurezza (non bisogna infatti affidare la carta a uno sconosciuto cameriere), «ma se all'esterno del ristorante in auto c'è un malfattore con un computer portatile e un'antenna, è anche possibile che i dati vengano trafugati nel momento stesso in cui il cliente li digita».

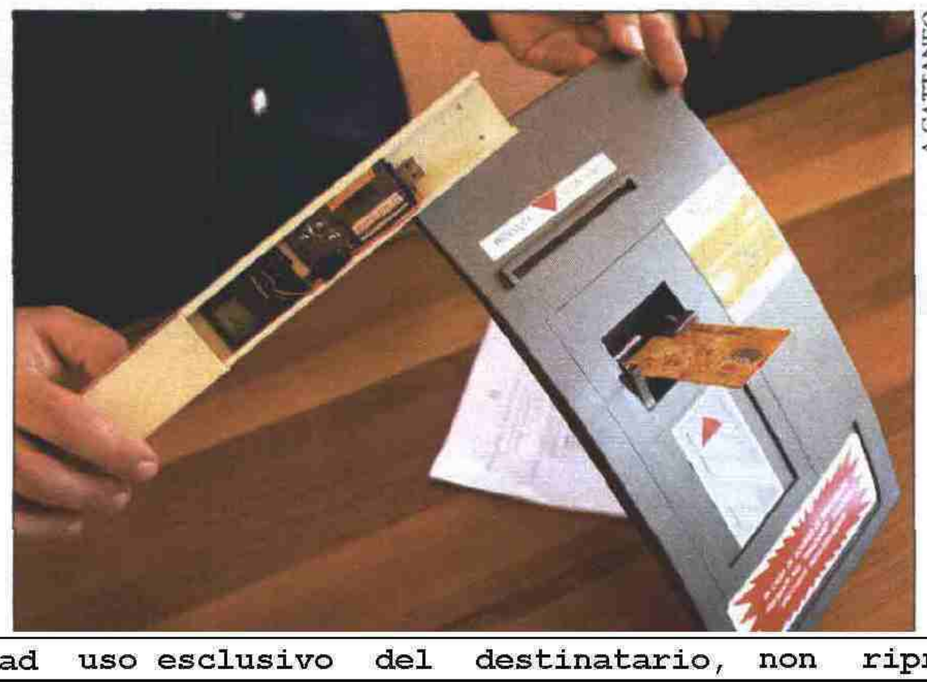
Per entrare in possesso dei numeri delle carte i nuovi criminali ricorrono a stratagemmi sempre nuovi. Alcuni rudimentali, ma efficaci. Trucchi che vengono battezzati da una nuova parola inglese che quasi sempre finisce con le tre lettere «ing». I due nuovi termini: «boxing» e «trashing». Il primo «ha la sua radice nella parola box, scatola, che è spesso usata anche nell'accezione di casella postale» racconta Lamberti. «Mail box è la cassetta delle lettere. La truffa indicata come boxing consiste nell'entrare in possesso di certe informazioni impadronendosi dell'estratto conto del titolare della carta o di altre comunicazioni che gli sono state inviate a proposito delle operazioni eseguite con la stessa».

Il criminale dunque viola la segretezza della corrispondenza e il suo obiettivo principale in questa fase è la casella della posta della sua vittima. In realtà non deve rubare le lettere, ma può «accontentarsi» di aprirle, ricopiare i dati che lo interessano, richiuderle e rimetterle al loro posto.

Un altro metodo (simile per il modo in cui i dati vengono sottratti, ma diverso rispetto ai tempi di recapito e lettura della posta) è quello del trashing. Poiché trash significa immondizia, è facile capire che «l'operazione consiste nel rovistare nella spazzatura» aggiunge Rapetto «cercando estratti conto, comunicazioni personali, indicazioni pratiche, segnalazioni che la banca o il network delle carte di credito ha spedito all'interessato. Tra i rifiuti, infatti, si possono recuperare scontrini, ricevute e altri tasselli utili a ricomporre quel puzzle che sono i dati della carta presa di mira. Ma lo avete mai letto uno scontrino di una spesa effettuata con carta di credito?» chiede retoricamente il finanziere. «Beh, fatelo, perché ci sono scritte tutte le informazioni che servono per effettuare un acquisto online, dal biglietto del treno a quello aereo.

«**Quindi un consiglio: non gettate mai lo scontrino nel cestino fuori del ristorante, ma custoditelo o distruggetelo.** Gli addetti ai lavori citano addirittura il "dumpster diving", ossia una specie di sport criminale che prevede immersioni nei cassonetti della spazzatura per recuperare ogni genere di dati che si possono ricavare da oggetti o altri rifiuti».

Tra i furbetti del digitale c'è anche chi semplicemente vuole risparmiare sulla bolletta del cellulare. «In aiuto dei tecnocriminali viene la tecnologia blueto-oth» spiega Rapetto «con un software e uno smartphone, ossia un cellulare con sistema operativo evoluto, si può telefonare addebitando la chiamata a uno sprovveduto che ha lasciato la funzione bluetooth accesa. Basta fare "cerca dispositivo", funzione disponibile in quasi tutti i cellulari in commercio, per vedere in ufficio o sul treno Eurostar quanti hanno il cellulare aperto agli intrusi». ●



A.CATTANEO

Panorama.it *Schede, prezzi, immagini di prodotti hi-tech: www.panorama.it/internet*