BSECURITY

IL PORTALE PIU' SICURO DI SEMPRE

Parola d'ordine: SICUREZZA

Benvenuto in questo spazio dedicato alla Sicurezza!

Gli uffici di **Sicurezza Logica**, **Sicurezza Informatica** (Security Operation Center + Nucleo Antifrodi), **Business Continuity** e **Sicurezza Fisica**, uniti in un percorso comune per realizzare uno strumento di aggiornamento, approfondimento e formazione nel settore della sicurezza in tutte le sue declinazioni.

La community nasce dall'esigenza di divulgare temi di security in modo semplice ed intuitivo, permettendo a tutti i nostri colleghi di arricchire il proprio bagaglio culturale con tematiche di assoluta rilevanza, sia per il proprio lavoro che per la vita privata. Non mancheranno inoltre, i nostri quiz per lavorare in sicurezza, rafforzando conoscenze teoriche e pratiche.

Il portale si pone come **punto d'incontro** per le sedi e le filiali, agevolando la ricerca di informazioni di proprio interesse e la fruizione di contenuti organizzati e di procedure operative sempre chiare ed aggiornate.

L'obiettivo è quello di sensibilizzare il personale sui rischi derivanti dalle minacce informatiche e trasferire loro il giusto senso di consapevolezza, in modo da garantire il giusto livello di sicurezza, sia per il Gruppo, che indirettamente per i clienti.

ULTIME NOTIZIE

E' ONLINE IL NUOVO BSECURITY MAGAZINE #10

In questo numero:

- Il data leak di Twitter
- I pericoli legati alle criptovalute
- La privacy nei moduli online

CAMPAGNA SMISHING VERSO LA CLIENTELA

Informiamo che negli ultimi giorni sono notevolmente aumentati gli attacchi di smishing nei confronti della clientela. La presente segnalazione ha l'obiettivo di condividere le informazioni sui temi di frode, in modo da garantire una corretta e proficua gestione della clientela e delle segnalazioni. Continua a leggere!

E' ONLINE IL NUOVO BSECURITY MAGAZINE #9

In questo numero:

- I Navigati - Informati e sicuri
- La tecnologia Blockchain: dai Bitcoin allo strumento di trasformazione digitale per il business delle imprese
- La Business Continuity

E' ONLINE IL NUOVO BSECURITY MAGAZINE #8

In questo numero:

- Chiavette USB in azienda? Meglio non usarle
- Cybercrime in Italia: rapporto 2022 sulla sicurezza ICT
- Cyberwar: gli impatti della crisi Russo - Ucraina

TRAFUGATE CARTE DI CREDITO SOSTITUTIVE

Si rende noto che sono pervenute diverse segnalazioni di carte di credito, spedite per posta al domicilio dei clienti, trafugate da ignoti malfattori. Si tratta di carte in rinnovo al 31 marzo 2022, nuove emissioni richieste tramite procedura wizard o carte richieste in sostituzione nel mese di febbraio 2022. Nel caso i clienti dovessero riferire di aver ricevuto telefonate apparentemente provenienti dalla Banca, è necessario verificare e bloccare eventuali carte in spedizione non ricevute e sospendere l'utenza SmartWeb. Continua a leggere!

L'IMPORTANZA DEI CONTROLLI ANTIFRODE

L'Ufficio Cybersecurity & Fraud Management monitora in tempo reale le transazioni sospette effettuate dai clienti tramite Smartweb e Corporate Banking (CBI). Durante lo svolgimento dei controlli di routine, necessitiamo di ingaggiare la Filiale di relazione del cliente oggetto di monitoraggio, per ricevere conferma o meno della genuinità della disposizione in osservazione. Continua a leggere!

CAMPAGNA MALWARE VIA EMAIL

Informiamo che nei primi giorni di febbraio, i nostri sistemi antispam hanno rilevato un aumento costante delle email malevole provenienti dall'esterno. L'email malevola si presenta con un nome mittente noto, ma con un indirizzo email sconosciuto. Il testo della mail contiene poche parole, tra cui il nome del file allegato e la password per aprirlo. Continua a leggere!

TELEFONATE DA FALSI CLIENTI

Informiamo che in questi giorni si sono verificati casi in cui le filiali ricevono telefonate apparentemente provenienti da clienti che si rivelano poi essere false, con l'obiettivo di ottenere informazioni sugli stessi. Continua a leggere!

IL VADEMECUM DEI CONTATTI:

- soc@bper.it - per questioni di sicurezza informatica (virus o anomalie di dispositivi aziendali)
- antiphishing@gruppobper.it - per segnalazioni di tentativi e/o casi concreti di phishing;
- frodionline@bper.it - in caso di frode su credenziali Smartweb;
- antifrodi@bper.it - in caso di frode su carte di debito;
- monitor_operativo@bibanca.it - in caso di frode su carte di credito o prepagate;

COME SEGNALARE UNA E-MAIL SOSPETTA:

Per segnalare **SPAM e PHISHING**, utilizzare le voci di menù presenti all'interno dell'email: "*Segnala come spam*" o "*Segnala come phishing*".

NON SEGNALARE MAI UNA EMAIL PROVENIENTE DA @BPER.IT!

I NOSTRI CONSIGLI

SECURITY OPERATION CENTER

Le minacce alla **sicurezza informatica** si evolvono costantemente, mettendo a rischio dati e risorse di singoli individui e aziende. Sapersi difendere è indispensabile per evitare brutte sorprese.

NUCLEO ANTIFRODI

Un uso responsabile degli strumenti di pagamento può rivelarsi l'arma giusta per difendersi dagli hacker ed evitare **sottrazioni fraudolente di denaro** dai propri conti correnti.

IL CONSIGLIO DEL GIORNO

Domande Frequenti

Cosa devo fare se ricevo un'email malevola al lavoro?

Il cliente è stato truffato, cosa devo fare?

Chi devo contattare se una persona sospetta si aggira nei pressi della filiale?

Glossario dei termini

Cos'è un ransomware? E perché è così pericoloso?

Qual è il significato di spoofing?

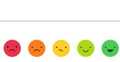
Qual è la differenza tra una truffa e una frode?

Mettiti alla prova!

Se hai già visto tutte le altre sezioni e ti senti sufficientemente preparato, mettiti alla prova!

Ti proporremo sfide interessanti per autovalutare il tuo livello di conoscenza di varie aree di sicurezza fisica ed informatica.

Cosa ne pensi della nostra community? Lascia un feedback!



Magazine

La rivista virtuale per la tua sicurezza

Le anime dell'area CISO unite per condividere l'importanza della *SICUREZZA*, mettendo in campo le proprie conoscenze ed esperienze.

Il nuovo Magazine non è semplicemente una rivista digitale, è soprattutto condividere e divulgare informazioni e opinioni di esperti, per mantenere al sicuro il nostro ambiente di lavoro ed il nostro spazio virtuale. Saranno pubblicati gli argomenti di maggior interesse con riferimenti a temi di attualità sul mondo della cyber security e della sicurezza fisica.

Per scoprire le novità e restare costantemente aggiornamento, ti consigliamo di consultare periodicamente il portale.

Sei interessato ad un argomento in particolare e vorresti che ne parlassimo nel prossimo numero? Compila il questionario.

In questo numero:

- DATA LEAK DI TWITTER
- I PERICOLI DELLE CRIPTOVALUTE
- LA PRIVACY NEI MODULI ONLINE

In questo numero:

- I NAVIGATI: Informati e sicuri
- LA TECNOLOGIA BLOCKCHAIN
- LA BUSINESS CONTINUITY

In questo numero:

- CHIAVETTE USB IN AZIENDA
- CYBERCRIME IN ITALIA: rapporto 2022 sulla sicurezza ICT
- CYBERWAR: gli impatti della crisi Russo - Ucraina

In questo numero:

- BRATA: l'App per Android che ruba dati bancari
- E-WALLET E PAGAMENTI DIGITALI: gestire transazioni in modo veloce e sicuro
- GOOGLE DORKS: migliorare le proprie ricerche su Google come farebbe un hacker

In questo numero:

- SMART WORKING IN SICUREZZA: Allontanare i rischi e proteggere la sicurezza della tua azienda
- IL VISHING: Attacchi telefonici e truffe online
- LE CAMPAGNE DI PHISHING: Saper riconoscere le attività sospette è fondamentale per non cadere in trappola

In questo numero:

- AUTENTICAZIONE A DUE O PIU' FATTORI: come proteggere i nostri account dalle intrusioni
- IL RANSOMWARE: aumenta la paura dopo il caso alla Regione Lazio
- POSTA ELETTRONICA CERTIFICATA (PEC): certificazione ed inalterabilità non sono sinonimo di sicurezza

In questo numero:

- TROJAN BANCARIO: Come proteggersi dal malware che svuota il conto corrente
- SPOOFING, L'APPARENZA INGANNA: Fingersi qualcun altro non è mai stato così semplice
- DARK WEB: Il listino prezzi dei dati rubati

In questo numero:

- DATA LEAK FACEBOOK: rubati i dati degli account di milioni di profili italiani e diffusi online
- IL PHISHING AI TEMPI DELLA PANDEMIA GLOBALE: gli attacchi informatici più diffusi
- AUTENTICAZIONE BIOMETRICA: sistemi biometrici per l'autenticazione, la sicurezza e l'accesso in filiale

In questo numero:

- LE PASSWORD: come proteggere i nostri dati e la nostra identità in modo sicuro
- SIM SWAP: cos'è, come funziona e come difendersi
- BEC FRAUD: sei sicuro che l'email ricevuta in ufficio sia autentica?

In questo numero:

- PHISHING: cos'è? come riconoscerlo? come proteggersi?
- TRUFFA SUBITO.IT: l'annuncio può rivelarsi una trappola
- PSIM: un modo più efficace ed efficiente di consolidamento della sicurezza di filiale

Magazine #10

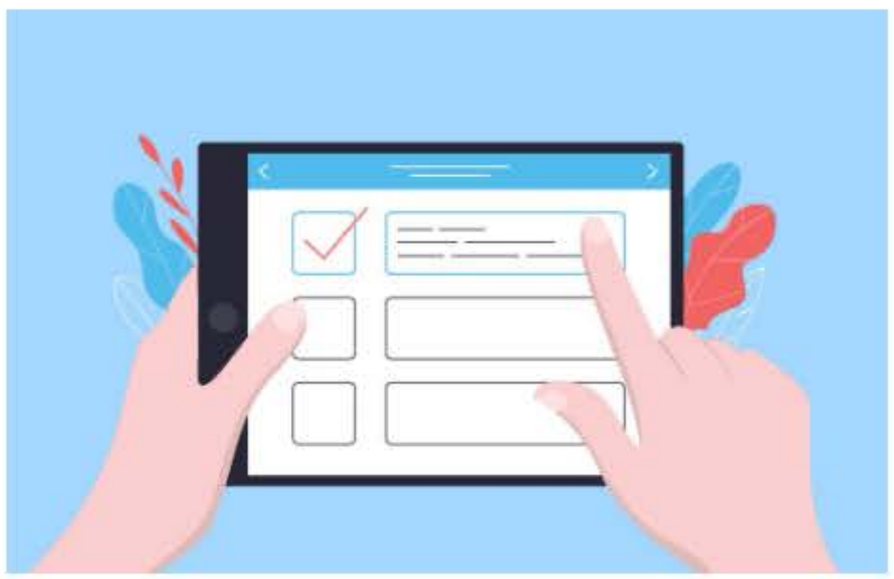
Sei interessato ad un argomento in particolare e vorresti che ne parlassimo nel prossimo numero? Compila il questionario.

Il data leak di Twitter

Attraverso un comunicato diffuso online, Twitter ha confermato che criminali informatici sono riusciti a raccogliere dati personali di alcuni utenti iscritti alla piattaforma social. La società non ha rivelato il numero di account coinvolti ma sono gli stessi aggressori ad indicarlo: si tratta di oltre 5,4 milioni di utenti su un totale di... Continua a leggere!

Le criptovalute

Abbiamo di recente parlato di Criptovalute, il cui mondo è letteralmente esploso. Le criptovalute, o criptocurrency, costituiscono una rete digitale semplice, sicura e funzionale che garantisce la tracciabilità e la verifica delle transazioni, pur rispettando la tutela degli utenti coinvolti. Tale tecnologia viene definita BLOCKCHAIN, in relazione alla modalità di archiviazione delle transazioni. Continua a leggere!



La compilazione dei moduli online

Da un recente studio portato avanti da ricercatori di tre università, una olandese, l'altra belga e l'ultima svizzera, emerge che un numero sorprendente di siti Web raccolga nostri dati o parte di essi mentre li digitiamo sul web, in moduli "che perdono dati", diventando così un altro metodo di raccolta dati, i quali vengono poi usati o fatti utilizzare a scopo pubblicitario. Per questo è importante accrescere la consapevolezza sul problema. Continua a leggere!

TWITTER CONFERMA LA FUGA DI DATI

Online le informazioni di 5,4 milioni di utenti

Cosa è successo?

Attraverso un comunicato diffuso online, **Twitter** ha confermato che criminali informatici sono riusciti a raccogliere dati personali di alcuni utenti iscritti alla piattaforma social. La società non ha rivelato il numero di account coinvolti ma sono gli stessi aggressori ad indicarlo: si tratta di oltre **5,4 milioni di utenti su un totale di 329 milioni di iscritti a Twitter**.

In base a quanto si apprende, a dicembre 2021, un gruppo hacker dichiarava di essere riuscito a raccogliere i dati personali di milioni di utenti Twitter sfruttando una vulnerabilità zero-day. Facendo leva sulla lacuna di sicurezza in questione, gli aggressioni hanno potuto interrogare Twitter inviando una lunga lista di numeri di telefono e indirizzi email. I server del social network hanno risposto, per ciascuna interrogazione, indicando se il numero di telefono o l'email trasmessa erano associati a uno specifico account.

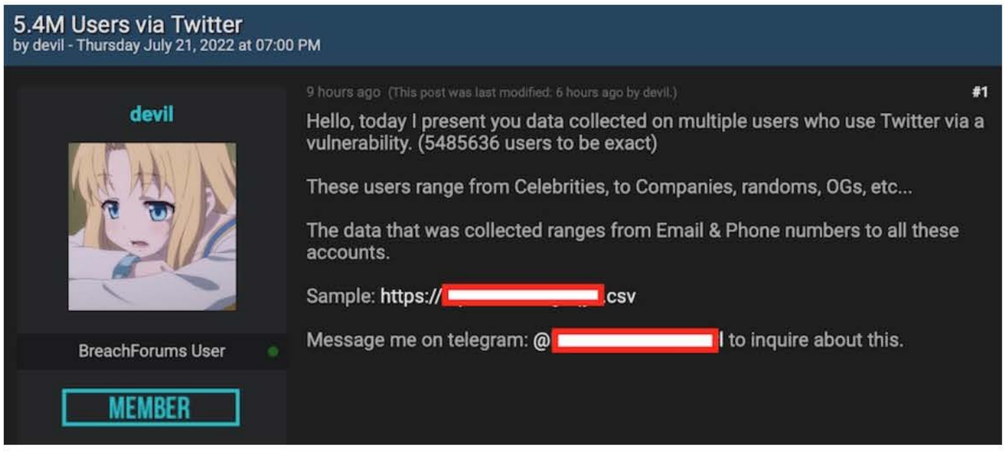
A questo punto è stato facile comporre un database contenente il nome corrispondente all'account Twitter, il numero di follower, informazioni di geolocalizzazione, indirizzo dell'immagine usata per il profilo e così via.

I dati sono già in vendita

Per quanto noto, un utente di nome "devil" ha messo in vendita con un annuncio su un noto forum del DARK WEB, un archivio contenente una massiccia collezione di dettagli su account Twitter. Come riferito dall'autore nell'annuncio stesso, si tratta per l'esattezza di 5.485.636 account. Una mole di dati enorme, se si pensa che ognuna di quelle righe è composta da venti colonne, tra le quali evidenziamo quelle relative ai dettagli come creazione dell'account, e-mail e numero di telefono. Il tutto comodamente formattato in un file CSV.

Gli autori di Restore Privacy, che hanno riportato per primi la vicenda, hanno contattato "devil" e sono riusciti a quantificare un prezzo per questa trattativa, non specificato nel thread del forum: i 5,4 milioni di account Twitter sono in vendita per 30.000 dollari.

Un po' come accaduto nel caso di una simile raccolta di dati che aveva interessato ben 100 milioni di account Facebook, anche il database relativo a Twitter contiene nomi di normali cittadini ma anche personaggi famosi e personalità di primo piano.



Ora che si fa?

Non è possibile identificare tutti gli account potenzialmente interessati, non ci sono misure da adottare da parte degli utenti e le password non sono state rubate.
Tuttavia, Twitter sta fornendo suggerimenti generali per proteggere gli account utente: "Per mantenere la tua identità al sicuro, ti consigliamo di non aggiungere un numero di telefono o un indirizzo e-mail pubblicamente noto al tuo account Twitter".
Ogni volta che si verifica una violazione dei dati, ci sono alcune cose che puoi fare per cercare di rimanere protetto.
Ecco alcuni suggerimenti:

- Modifica immediatamente i tuoi dati di accesso, come la password o il nome utente. Questa è la migliore difesa contro una violazione dei dati.
- Usa password uniche e complesse per ogni account online che gli hacker non possono facilmente indovinare. Prova a utilizzare un gestore di password per creare e memorizzare i tuoi dati. (Ne abbiamo parlato qui)
- Ove offerto, utilizzare l'autenticazione a due fattori (2FA). Ciò aggiunge un altro livello di protezione in cui è necessario autenticare il proprio accesso tramite un dispositivo secondario. (Ne abbiamo parlato qui)
- Fai attenzione alle email di phishing che affermano di avere dettagli sulla violazione dei dati di Twitter. Fare clic su collegamenti o scaricare allegati da e-mail indesiderate potrebbe infettare il dispositivo con malware o causare altri problemi di sicurezza informatica. (Ne abbiamo parlato qui)

Per concludere, quali sono i maggiori rischi da cui proteggersi?

- *rischi per me*: che mi truffino, ingannino o danneggino la mia reputazione;
- *rischi per gli altri*: qualcuno potrebbe guadagnare la fiducia della vittima attraverso il mio account oppure utilizzare l'account per scopi climinali;
- *rischi di sospensione* legati all'uso non conforme alle regole di Twitter.

Conoscendo cosa si rischia si può fruire di un'esperienza gratificante e anche utile professionalmente, nel caso ci interessi questo aspetto.