RICONOSCERE I TENTATIVI DI PHISHING: TRAINING PER I DIPENDENTI DI UNA BANCA

RAVNAQ-BANK

HWG Sababa

Ravnaq Bank

Fornisce servizi bancari ad imprese e consumatori dal 2001

L'headquarter si trova a Tashkent

150 specialisti

È la prima banca in Uzbekistan a lanciare i pagamenti contactless via smartphone

"Siamo consapevoli della necessità di dover adottare misure complesse per affrontare i rischi cyber. Queste includono il monitoraggio continuo della sicurezza, un piano di risposta agli incidenti e la formazione degli utenti per ridurre al minimo gli errori umani ed aumentare la resilienza complessiva della banca"

Abdukakhor Tulyaganov,
Capo della Sicurezza della Banca.

Oltre ad essere tra le principali minacce informatiche in Europa, il phishing rappresenta un problema importante anche per le aziende dei Paesi dell'Asia Centrale. Sulla strada della trasformazione digitale, i cyber criminali sfruttano ogni opportunità per insinuarsi nelle reti aziendali. Per esempio, inducono gli utenti a condividere le proprie credenziali o commettere altri errori critici.

Per indurre le persone a compiere azioni insicure, i criminali informatici manipolano le loro emozioni. Secondo il recente HWG Sababa Awareness Report, sono l'avidità, la curiosità e il desiderio di aiutare – uniti al senso di urgenza o all'autorità del mittente – che spingono le persone ad agire, più di ogni altra cosa. Pertanto le aziende, soprattutto quelle che operano in settori strategici come quello finanziario, si impegnano a formare i propri dipendenti per dotarli delle conoscenze e delle competenze necessarie per riconoscere, filtrare e segnalare qualsiasi comunicazione sospetta.

Questo approccio consente di sfruttare il fattore umano a vantaggio dell'organizzazione, trasformando i dipendenti in un ulteriore elemento di protezione per l'azienda stessa e per i clienti. Questo è ciò che ha saputo riconoscere e comprendere tempestivamente anche Ravnaq Bank.

Sfide e obiettivi del progetto

Operativa da oltre 20 anni, Ravnaq Bank è una banca moderna ed innovativa. Ha la sua sede principale a Tashkent e non possiede altre filiali poiché tutte le operazioni bancarie avvengono virtualmente. È stata infatti una delle prime banche in Uzbekistan ad aver lanciato un'applicazione per smartphone per le operazioni bancarie online e l'e-commerce, velocizzando e semplificando il business di diversi clienti in tutto il Paese, tra cui grandi produttori alimentari e organizzazioni sanitarie.

L'innovazione digitale ha comportato un ripensamento sull'approccio alla sicurezza della banca. Due anni fa, quando Ravnaq Bank ha rilasciato la sua applicazione, il team IT ha condiviso le responsabilità legate alla cybersecurity con il dipartimento dedicato alla sicurezza fisica della banca. Valutati i rischi legati alla trasformazione digitale, la banca ha riconosciuto l'importanza di sensibilizzare i propri professionisti in materia di sicurezza.

[1] Rapporto Clusit sulla Sicurezza Informatica 2022
[2] HWG Sababa Awareness Report 2021

“Durante una delle attività di assessment interno abbiamo notato vari problemi tra gli utenti. Tra questi, l'utilizzo di password elementari per accedere a computer e smartphone, la quasi totale mancanza di nozioni di base di cyber security personale - come bloccare il PC quando ci si allontana dalla scrivania - ed errori nel trattamento dei dati dei clienti”,

ha commentato Abdukakhor Tulyaganov, Capo della Sicurezza della Banca,

“Ovviamente abbiamo una policy di sicurezza che aggiorniamo ed approviamo mensilmente con il Cybersecurity Center dell'Uzbekistan, ma oltre a tenere sotto controllo la situazione con le policy, abbiamo deciso di concentrarci anche sulla formazione dei nostri specialisti”.

Il progetto

Ravnaq Bank si è subito resa conto che la formazione richiede conoscenze, competenze specifiche e tempo, rappresentando quindi un carico di lavoro eccessivo per solo 2 specialisti. Pertanto, il team dedicato alla sicurezza ha deciso di unire le forze con il dipartimento IT e il team di formazione ed insieme hanno convinto il Consiglio di Amministrazione a sostenere l'investimento nell’awareness appoggiandosi ad un partner esterno.

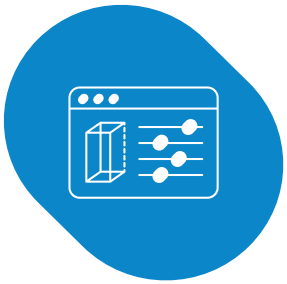
“Non ci abbiamo messo molto tempo a scegliere un corso offline. La nostra esperienza ci ha dimostrato che spesso i training mancano di una formazione pratica continua e noi avevamo bisogno di una soluzione che non distraesse i dipendenti dal lavoro, che fosse facile da usare – soprattutto nelle ore mattutine – e che rinfrescasse le conoscenze degli utenti ogni 3 mesi. Inoltre, per noi era importante poter formare i nostri specialisti in uzbeko e in russo”,

ha spiegato Abdukakhor Tulyaganov,

“Ecco perché siamo stati molto felici di conoscere HWG Sababa”.

Una delle ragioni principali che hanno fatto ricadere la scelta della Banca su HWG Sababa è la combinazione dei suoi moduli di formazione generici e specifici con simulazioni di attacchi di phishing:

I moduli generici sono universali e adatti a fornire ai professionisti nozioni base sull'uso corretto di computer e dispositivi mobili e su come lavorare online in sicurezza.



I moduli specifici sono rivolti ai dipendenti di determinati team (ad esempio, assistenza tecnica, marketing e altri) e sono volti a sviluppare competenze in materia di cybersecurity all’interno di scenari comuni e attività quotidiane svolte dai professionisti.

Le **simulazioni di attacchi di phishing** consentono ai dipendenti di un qualsiasi team della banca di affinare le proprie competenze pratiche acquisite durante la formazione. Nell'ambito del progetto, Ravnaq Bank ha deciso di condurre simulazioni di attacchi di phishing ogni 3 mesi.

Un fattore importante nella scelta della soluzione è stata anche la disponibilità dei moduli di training in uzbeko e russo. Spesso gli sviluppatori di soluzioni di sicurezza impiegano molto tempo per la localizzazione uzbeka. In questo progetto invece, HWG Sababa non solo ha tradotto tutti i materiali del corso, ma ha anche adattato la piattaforma al look&feel aziendale di Ravnaq Bank, garantendo un'esperienza formativa ottimale per tutti gli specialisti della banca.

Test della piattaforma

Prima di procedere con il progetto, Ravnaq Bank ha deciso di testare la piattaforma su un piccolo gruppo di utenti. La POC (Proof of Concept) è durata una settimana.

"Abbiamo simulato un attacco di phishing per testare la preparazione generale dei nostri colleghi nel reagire ad un attacco informatico. È stata una bella sorpresa perché i nostri dipendenti si sono comportati meglio del previsto. Solo pochi di loro hanno compiuto azioni insicure di fronte all'e-mail di prova, mentre la maggior parte ha chiamato immediatamente il supporto tecnico per segnalare la ricezione di messaggi sospetti",

ha raccontato Abdukakhor Tulyaganov,

"Il risultato della simulazione è stato positivo, quindi abbiamo deciso di procedere con il progetto".

Risultati

Ravnaq Bank ha adottato un piano di implementazione graduale dei corsi di formazione per i dipendenti:

In primo luogo, era prevista la formazione dei team IT e di sicurezza, in modo che fossero pronti a supervisionare a loro volta la formazione di altri colleghi

In seconda battuta, era prevista la formazione del team retail, che lavora con i clienti fisici e i loro dati, l'app di mobile banking e le carte di credito

L'esperienza di Ravnaq Bank dimostra l'importanza di un approccio strategico verso le tecnologie innovative e la loro applicazione sicura dal punto di vista informatico. Investendo nella formazione dei dipendenti, le aziende non solo riducono i rischi di sicurezza riconducibili all'errore umano, ma creano anche un ulteriore livello di protezione per il loro business.

"I tentativi di frode e di phishing stanno crescendo in modo esponenziale, soprattutto nei fine settimana e a tarda notte. Pertanto, siamo consapevoli della necessità di dover adottare misure complesse per affrontare i rischi cyber",

ha concluso Abdukakhor Tulyaganov,

"Queste includono il monitoraggio continuo della sicurezza, un piano di risposta agli incidenti e la formazione degli utenti per ridurre al minimo gli errori umani ed aumentare la resilienza complessiva della banca".

HWG Sababa

RAVNAQ-BANK

Follow us on:

www.hwgsababa.com