ODPOČINOK VÁS MÔŽE VYJSŤ DRAHO

PODVODY PRI REZERVÁCII UBYTOVANIA

Plánovanie dovolenky je spojené s očakávaním a radosťou. Práve v tomto rozpoložení sme menej ostražití – a to útočníci dobre vedia. Podvody cielené na dovolenkárov a zákazníkov rezervačných portálov patria k najrýchlejšie rastúcim formám online podvodov. Útočníci nepotrebujú preniknúť do systémov banky ani získať heslá hrubou silou. Stačí im napodobniť dôveryhodný e-mail, vytvoriť falošnú platobnú stránku a využiť moment, keď obeť práve potvrdila rezerváciu a čaká na ďalšie pokyny.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Mechanizmus podvodu pri rezervácii ubytovania

Útočníci aktívne monitorujú rezervačné portály alebo priamo kompromitujú účty ubytovacích zariadení na platformách ako Booking.com, Airbnb či podobných službách. Po úspešnej rezervácii môže hosť obdržať e-mail, SMS alebo správu priamo v chatovacej aplikácii platformy, ktorá sa na prvý pohľad javí ako legitímna komunikácia od ubytovania alebo samotného portálu.

Podvodná správa najčastejšie predstiera potvrdenie rezervácie alebo výzvu na uhradenie platby. Jej dizajn verne kopíruje vizuálny štýl známych rezervačných platforiem – logo, farby, formát textu. Práve táto vizuálna podobnosť robí tieto podvody obzvlášť záludnými a ťažko rozoznateľnými od autentickej komunikácie.

Cieľom podvodnej správy je získať niektorú z nasledujúcich hodnotných informácií: kompletné údaje z platobnej karty vrátane čísla karty, dátumu exspirácie a CVV kódu, a to často spolu s kódom na pridanie karty do mobilnej peňaženky Apple Pay alebo Google Pay. Útočníci môžu rovnako žiadať prihlasovacie údaje do zákazníckeho účtu na rezervačnom portáli, kde má obeť uloženú platobnú kartu, alebo priamo vyzvať na bankový prevod na zaslaný IBAN.

Správa zvyčajne obsahuje odkaz na podvodnú webovú stránku, ktorá napodobňuje originálnu platformu, alebo priamo platobné údaje na prevod. Útočníci pri tvorbe týchto stránok používajú domény s drobnými preklepmi alebo znakmi navyše v URL adrese – napríklad booking-secure.com namiesto booking.com. Rovnako podozrivé môže byť meno odosielateľa v e-mailovej adrese, ktoré nevyzerá ako oficiálna doména danej platformy.

Neoddeliteľnou súčasťou útoku je vyvolanie pocitu naliehavosti a časovej tiesne. Správa upozorňuje, že rezervácia bude zrušená, ak platba neprebehne do stanoveného termínu – zvyčajne v priebehu hodín. Tento tlak obeť núti konať rýchlo a bez dostatočného overenia, čo je presne to, čo útočník potrebuje.

Indikátory podvodu pri rezervácii ubytovania

Prvým varovným signálom je správa, ktorá žiada platbu alebo citlivé údaje a prichádza mimo štandardných komunikačných kanálov – napríklad priamo do osobnej správy alebo e-mailom s neoficiálnou adresou odosielateľa. Legitímne rezervačné platformy komunikujú výhradne cez overené systémové notifikácie a nikdy nepožadujú opätovné zadanie platobných údajov po uskutočnení rezervácie.

Pozornosť venujte URL adrese stránky, na ktorú vás správa presmerúva. Autentická doména by mala presne zodpovedať oficiálnej adrese platformy. Akýkoľvek preklep, číslo navyše, pomlčka alebo iná neobvyklá prípona sú silným indikátorom phishingovej stránky. Prehliadač vás môže tiež upozorniť na neoverený bezpečnostný certifikát.

Žiadosť o CVV kód, kód pre Apple Pay alebo Google Pay je mimoriadne závažným varovným signálom. Legitímna platobná brána tieto kódy po zadaní nikdy neukladá ani nepožaduje opakovane. Takisto platí, že priamy bankový prevod na IBAN ako jediná možná forma platby za ubytovanie je nezvyčajná a väčšina dôveryhodných platforiem túto možnosť ako primárnu neuplatňuje.

Každá správa zo súkromnej komunikácie, v ktorej neznáma osoba žiada citlivé údaje alebo prevod peňazí, by mala byť automaticky považovaná za podozrivú. Platí to aj v prípade, ak sa odosielateľ identifikuje ako zamestnanec ubytovania alebo zákaznícka podpora platformy.

Ako sa chrániť pred podvodmi pri rezervácii ubytovania

Základom ochrany je pristupovať k zákazníckemu účtu vždy len cez oficiálnu webovú stránku alebo aplikáciu, ktorú dlhodobo používate a ktorú máte uloženú v prehliadači alebo na ploche zariadenia. Nikdy neklikajte na prihlasovací odkaz z e-mailu alebo správy – adresu zadajte ručne alebo použite záložku.

V prípade pochybností o pravosti platobnej výzvy si jej oprávnenosť overte priamo u poskytovateľa ubytovania – telefonicky alebo cez overený komunikačný kanál na platforme. Nezavolajte na číslo z podozrivej správy, ale vyhľadajte kontakt na oficiálnej stránke.

Pri online platbách za ubytovanie zvážte použitie jednorazovej virtuálnej karty, ktorú si môžete vygenerovať priamo v bankovej aplikácii. Nastavte na nej internetový limit len mierne vyšší, než je suma rezervácie, a po uskutočnení platby limit opäť znížte alebo kartu deaktivujte. Tým výrazne obmedzíte potenciálnu škodu v prípade, že by útočník získal číslo karty.

Ak máte podozrenie, že vaše platobné údaje mohli byť kompromitované alebo že ste sa stali obeťou podvodu, bezodkladne kontaktujte svoju banku. Požiadajte o zablokovanie karty a iniciovanie reklamačného konania. Rýchla reakcia výrazne zvyšuje šancu na vrátenie finančných prostriedkov.

Podvody pri rezervácii dovolenky sú dômyselne navrhnuté tak, aby zneužili moment radosti a očakávania, keď je naša opatrnosť prirodzene znížená. Vizuálna dôveryhodnosť podvodných správ ich robí obzvlášť záludnými. Pravidelné overovanie URL adries, odmietnutie konať pod časovým tlakom a používanie virtuálnych kariet sú pritom jednoduché návyky, ktoré dokážu efektívne ochrániť vaše financie pri každej ďalšej rezervácii.