

Ahoj, pro zajímavost a hlavně pro varování kamarádů, jsem zdokumentoval, jak se ze mě pokusili vylákat přístupové údaje k bankovnímu účtu.

Odborně se tomu říká útok přes sociální inženýrství, phishing. Více když tak na Wikipedii: [https://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_in%C5%BEen%C3%BDrstv%C3%AD_\(bezpe%C4%8Dnost\)](https://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_in%C5%BEen%C3%BDrstv%C3%AD_(bezpe%C4%8Dnost))

Chtěl jsem prodat CB anténu, co jsem před časem koupil, ale nakonec jsme jí nepoužili.

1. Zadal jsem inzerát na www.bazos.cz na anténu.
2. Po několika hodinách mě kontaktoval první zájemce. Už to bylo podezřelé, anténa je dost specialita, že by si toho někdo všiml tak rychle?
3. Adresa odesílatele byla annnannowakjka1928@gmail.com. Že by 94-letá babička s polským jménem měla zájem o anténu?

From: annnannowakjka1928@gmail.com <annnannowakjka1928@gmail.com>

Sent: Wednesday, March 15, 2023 11:20 AM

To: filip@weber.cz

Subject: Bazos.cz - odpoved na inzerat 166051046 - antena CB + prislusenstvi

Dobrý den váš inzerát ještě aktuální?

annnannowakjka1928@gmail.com - Email byl odeslan ze serveru Bazos.cz.

4. Bylo mi to jasné kolik bije, divná adresa, špatný slovosled, chybí sloveso, ale zajímalo mě to, tak jsem odpověděl.

st 15. 3. 2023 v 11:25 odesílatel <filip@weber.cz> napsal:

F: Dobrý den, ano platí, inzerát jsem podal asi před třemi hodinami.

K vyzvednutí Praha nebo pošlu přes Zásilkovnu za 120,-. Vše je originál zabaleno v krabici z obchodu.

Proběhl ještě dotaz na stav: Stav je dobrý? (Psal v inz., že je to nové....) Odpověď: Nové, nepoužité.

5. Mezitím mi dorazily podobné emaily:

Dobry den, mam zajem ale jsem z kladna... nejezdite nahodou na Kladno? Ja bych mohl prijet az o vykend...

humlik88@seznam.cz - Email byl odeslan ze serveru Bazos.cz. (Podle češtiny zase podvod, ale odpoledne mi dokonce zavolaal, možná fakt zájemce, prý o víkendu přijede. Uvidím, třeba se z toho ještě něco zajímavého vyklube). Takže podle špatné češtiny nelze posuzovat.

Zdravim Vas mal by som zaujem o antenu. Vedeli by ste to poslat na Slovensko napr cez Packetu ? Ja by som vam dopredu vedel poslat peniaze na ucet.

S pozdravom Marek.

markoo.mt@gmail.com - Email byl odeslan ze serveru Bazos.cz.

Dobrý den! Mám zájem o váš inzerát , prosím, odpovězte mi e-mailem. Domluvíme se na vyzvednutí. Děkuji Jakub.

kuba2017cr@seznam.cz - Email byl odeslan ze serveru Bazos.cz.

(Psal by normální člověk, mám zájem o inzerát? Ne! Psal by mám zájem o anténu.)

A dalších několik podobných, je možné, že jsou mezi nimi i opravdoví zájemci. Ale nemyslím.

4. Babička komunikovala dál:

*Anna: Jsem z Plzně, mohu si objednat kurýrní službu Dpd " Platbu obdržíte před odesláním.
Vyhovuje vám to? ☺ ☺ ☺*

F: Lepší by byla ta Zásilkovna, kam to prostě ráno dovezu a pošlou to na dobírku. Vy při převzetí zaplatíte kartou a oni mi pak peníze pošlou.

Anna: DPD je velmi jednoduché: zaplatím za doručení a zboží, vy musíte dostat peníze na svůj účet prostřednictvím DPD a potvrdit doručení, jakmile jsou peníze na vašem účtu, kurýr vás kontaktuje a vyzvedne zboží podle vašeho přání ☺

F. Dobře, moc se mi to nehodí, ale pošlu to tedy DPD.

5. Pozor blíží se vyvrcholení:

*st 15. 3. 2023 v 14:05 odesílatel Anna Nowak <annnannowakjka1928@gmail.com> napsal:
Dobře, nyní vytvořím platbu prostřednictvím DPD a pošlu vám formulář pro příjem prostředků,
obdržíte peníze po dobu 5 minut .*

Další zpráva:

http://dpd.info517630.online/?get&track_id=33787140

Zaplatila jsem ☹️ Chcete-li obdržet peníze, přejděte na odkaz a potvrďte objednávku.

6. Super, mám link s potvrzením platby. Link je jasně fake (dpd.info517630.online), ale toho si běžný uživatel (BFU) nevšimne.

https://dpd.info517630.online/?get&track_id=33787140

Poslat balíkČekám balíkO násSpolečenská odpovědnostDPD ShippingMoje DPDPodpora

Výzkum chování zákazníků na internetu

E-shopper Barometer 2021

Kde je moje zásilka?

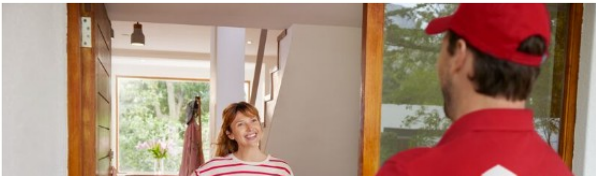


Pro sledování zásilky

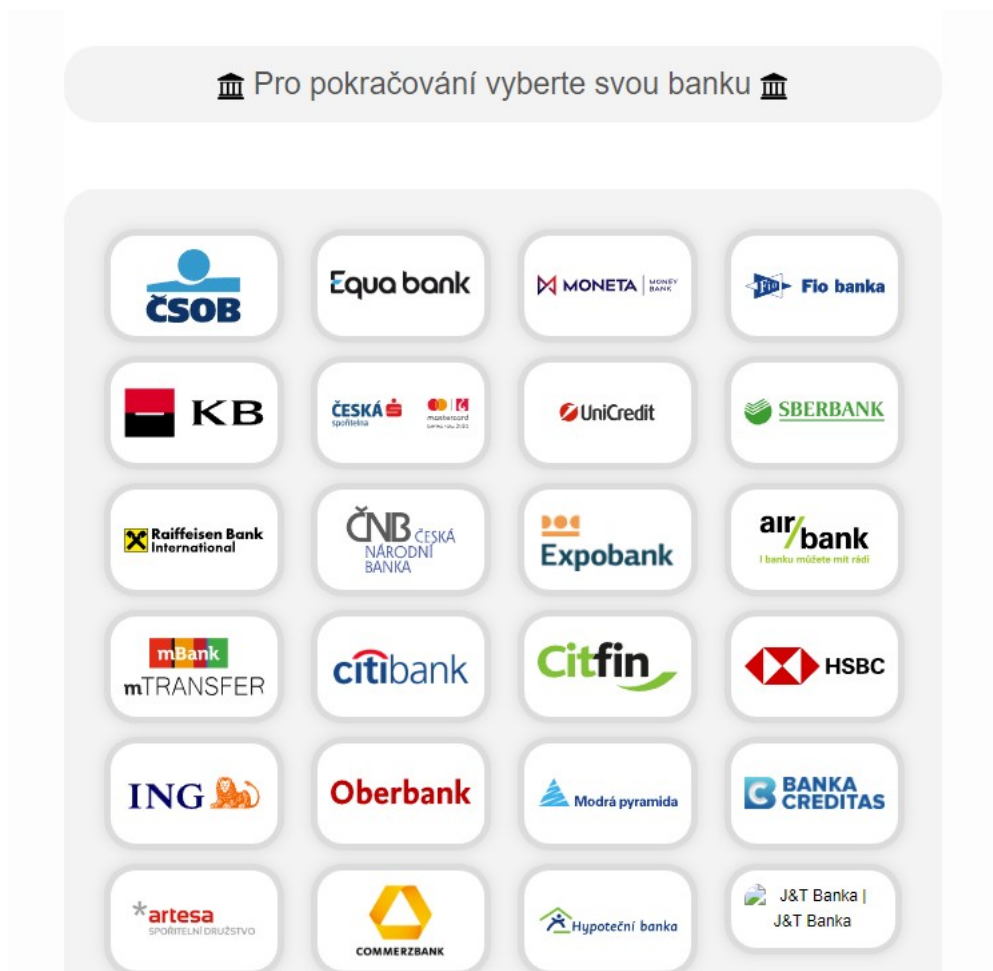
JMÉNO KUPUJÍCÍHO	Anna Novak
PRODUKT	AIRSPY mini + antena + příslušenství
CENA	3000,00 Kč
DORUČOVACÍ ADRESA	nám. Republiky 1306 32 Plzeň Česko
ČÍSLO DOPRAVY	33787140

[POKRAČOVAT](#)

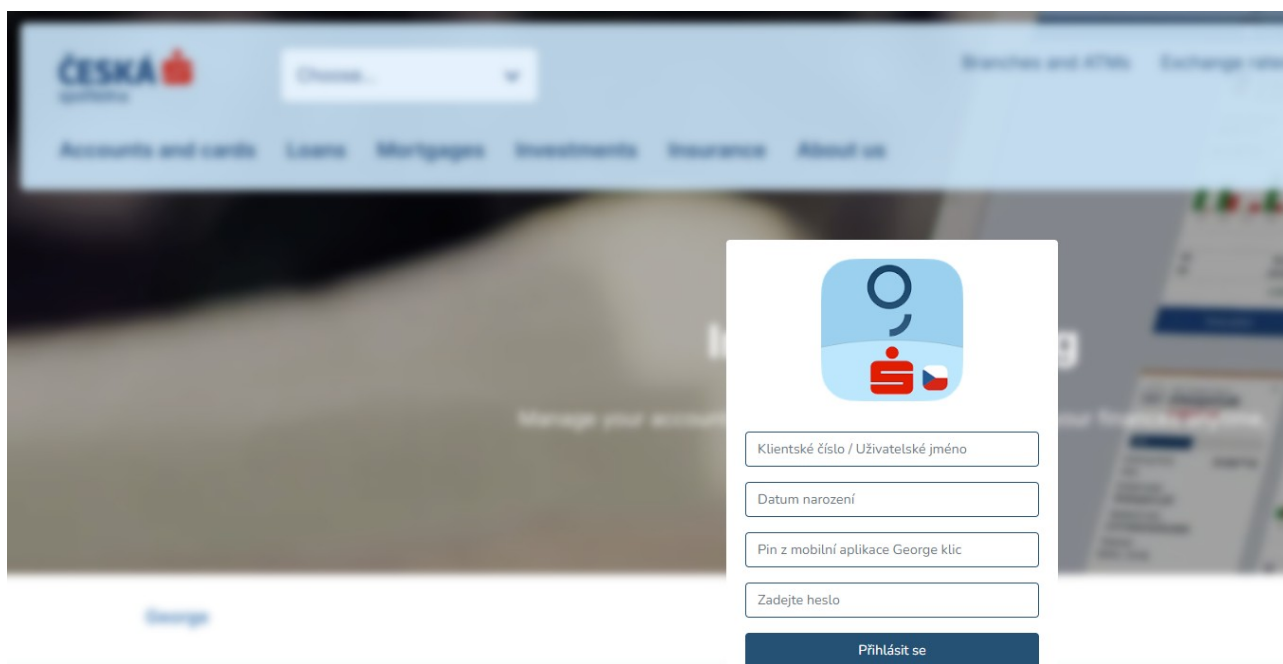
Predict - S námi víte na hodinu přesně, kdy přijedeme



7. jsem lačný po penězích, tak klikám na POKRAČOVAT
https://dpd.info517630.online/banks?track_id=33787140



7. Vybírám třeba Českou spořitelnu:



8. Začíná to být napínavé! Zadávám smyšlené údaje a pokračuji. Chce to po mě číslo karty.

A screenshot of the dpd payment form. At the top is the dpd logo. The form has two main input fields: 'Číslo karty' (Card number) and 'Jméno na kartě' (Name on card). The card number field contains the text '5689 4023 7643 5890'. The name field contains 'POLIB MI'. Below these fields is a dark green button labeled 'POKRAČOVAT'. At the bottom of the form, there is a security notice: 'HTTPS / SSL Bezpečné připojení' with a lock icon. Below this are logos for 'VERIFIED by VISA' and 'MasterCard SecureCode'.

9. Dostávám další výzvu:

Sl

Web dpd.info517630.online říká

Vaše banka požádala o dodatečné ověření. Vyplňte všechna další pole a zkuste to znovu.

OK

Jméno na kartě

POLIB MI

POKRAČOVAT

HTTPS / SSL Bezpečné připojení

VERIFIED by VISA MasterCard SecureCode

10. Mám pro strach uděláno, přejel jsem Saharu i Gobi na motorce, tak zadávám datum expirace a CVC. Důvěryhodné, že?!



Číslo karty

5689 4023 7643 5890

Jméno na kartě

POLIB MI

Datum vypršení platnosti CVC/CVV kod

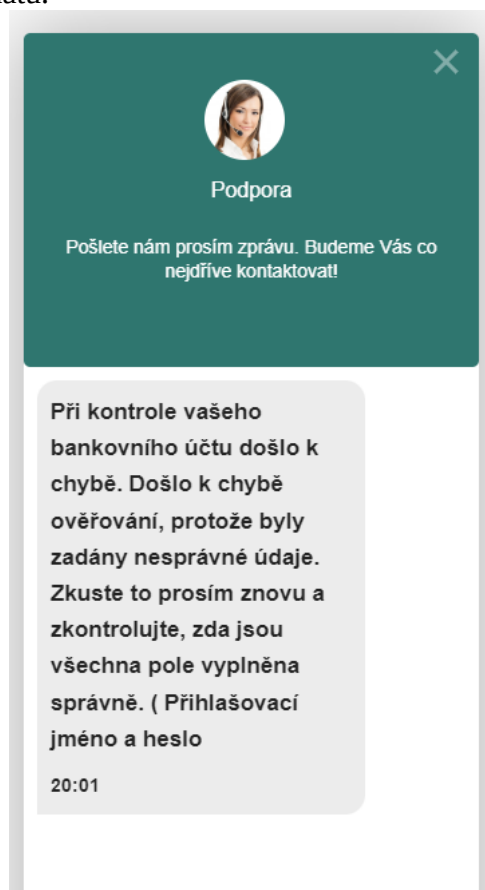
10/24

POKRAČOVAT

HTTPS / SSL Bezpečné připojení

VERIFIED by VISA MasterCard SecureCode

11. Vyskočila na mě postupně okna Platba zamítnuta, zadejte znova heslo. Z banky mi asi chtějí pomoci a tak mě vyzývají k chatu.



Dál mě to nepustilo, škoda, docela jsem se bavil. Tak alespoň posílám posílám babičce zpět pozdrav:

Děkuji za spolupráci, přeposílám váš kontakt POLICII. Včetně vaší IP adresy a všech identifikátorů z komunikace.

Vždy ve střehu!

Koukejte do hlavičky linku a zamyslete se – <https://.....>

Do banky se přihlašujte přes oficiální stránky banky, ne přes poslané linky.

Vždy mějte dvoufaktorové ověření přes aplikaci, NE PŘES SMS.

Nikdy nikam nezadávejte číslo karty a CVC, když si nejste fakt jisti.

Tohle nevím jistě, ale – používejte kreditní, nikoliv debetní kartu. Kreditní má limit a je tam čas na zablokování platby. U debetní se strhává přímo z účtu a účet jde tak vysát.

Ta komunikace už nejspíše byla generována umělou inteligencí!

Jirka z CompuNet mi ještě v rekaci napsal:

„Dnes jsem se setkal se zajímavým phishingem města Kralup.

Zveřejnili příspěvek o tom, kdy otevřou bazén po rekonstrukci s odkazem na web s otevírací dobou.

Link v pořádku, po najetí myší to ukazovalo správný web, ale po kliknutí se otevřela stránka, kde mě to ukázalo info o mém ISP (z ripe) a že jsem vyhrál iPhone, se spoustou komentářů lidí, co psali že zaplatily jen poštovné a iPhone už je doma. A odkaz na zadání čísla karty, data a CVC...

Bud' má člověk, co to vkládá, vir nebo jim někdo ukradl přístup do publikačního systému (většinou WordPress) a upravuje příspěvky po zveřejnění.“

Tak opatrně!

Filip Weber, weber@compunet.cz, březen 2023