Příklady pro Scénář 6: „Phishing detektivové“

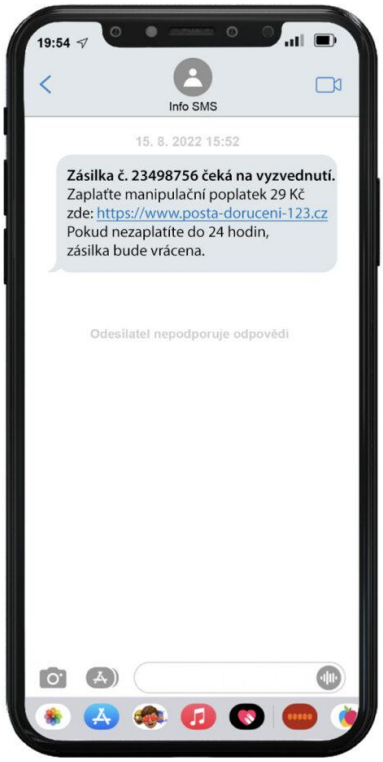
Připravili jsme pro Vás sadu praktických příkladů phishingových útoků, které můžete využít během společné **Rodinné Kyberchvíle**. Cílem je ukázat si na konkrétních situacích, jak vypadají nejčastější online podvody – a naučit se je včas rozpoznat.

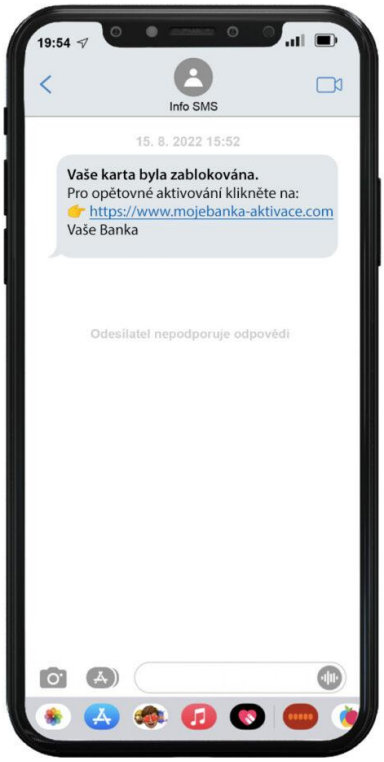
Phishing, smishing nebo vishing jsou hrozby, se kterými se může setkat každý člen rodiny – dítě, rodič i prarodič. Společným tréninkem posílíte nejen svou **kybernetickou bezpečnost**, ale i důvěru a otevřenou komunikaci v digitálním světě.

Příklady podvodných sms (smishing)

Smishing je forma phishingového útoku, která probíhá prostřednictvím SMS zpráv. Útočník se v nich vydává za důvěryhodnou osobu nebo instituci (např. banku, kurýra, úřad) a snaží se vylákat osobní údaje, hesla, přístupové kódy nebo přimět oběť k kliknutí na škodlivý odkaz.

Smishingové zprávy často vzbuzují naléhavost – tvrdí, že je potřeba rychle ověřit platbu, doručit balík nebo zablokovat účet. I když vypadají důvěryhodně, jejich cílem je oklamat a vylákat údaje nebo instalovat škodlivý software. Níže uvádíme několik typických scénářů, na které si dát pozor.

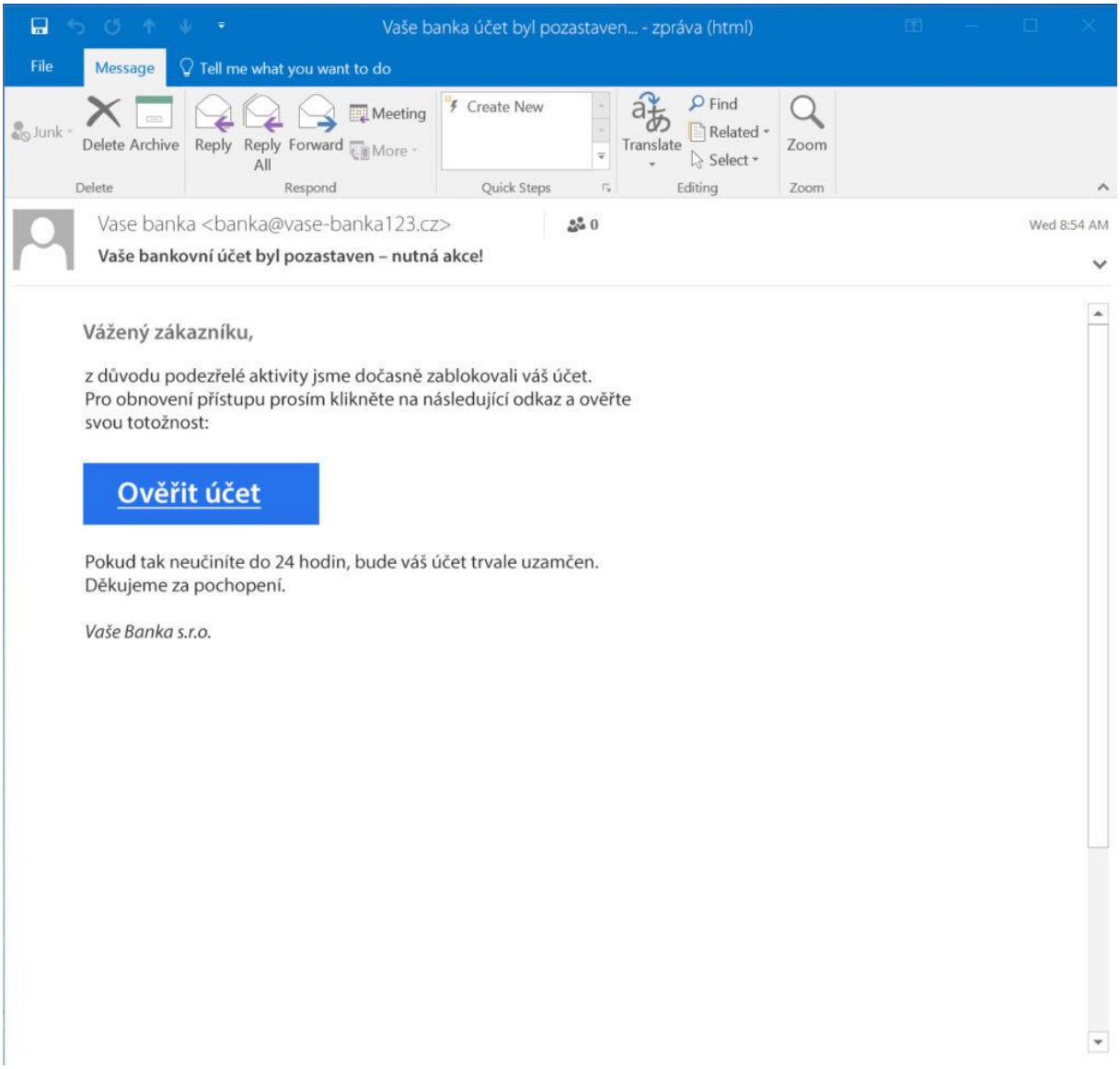




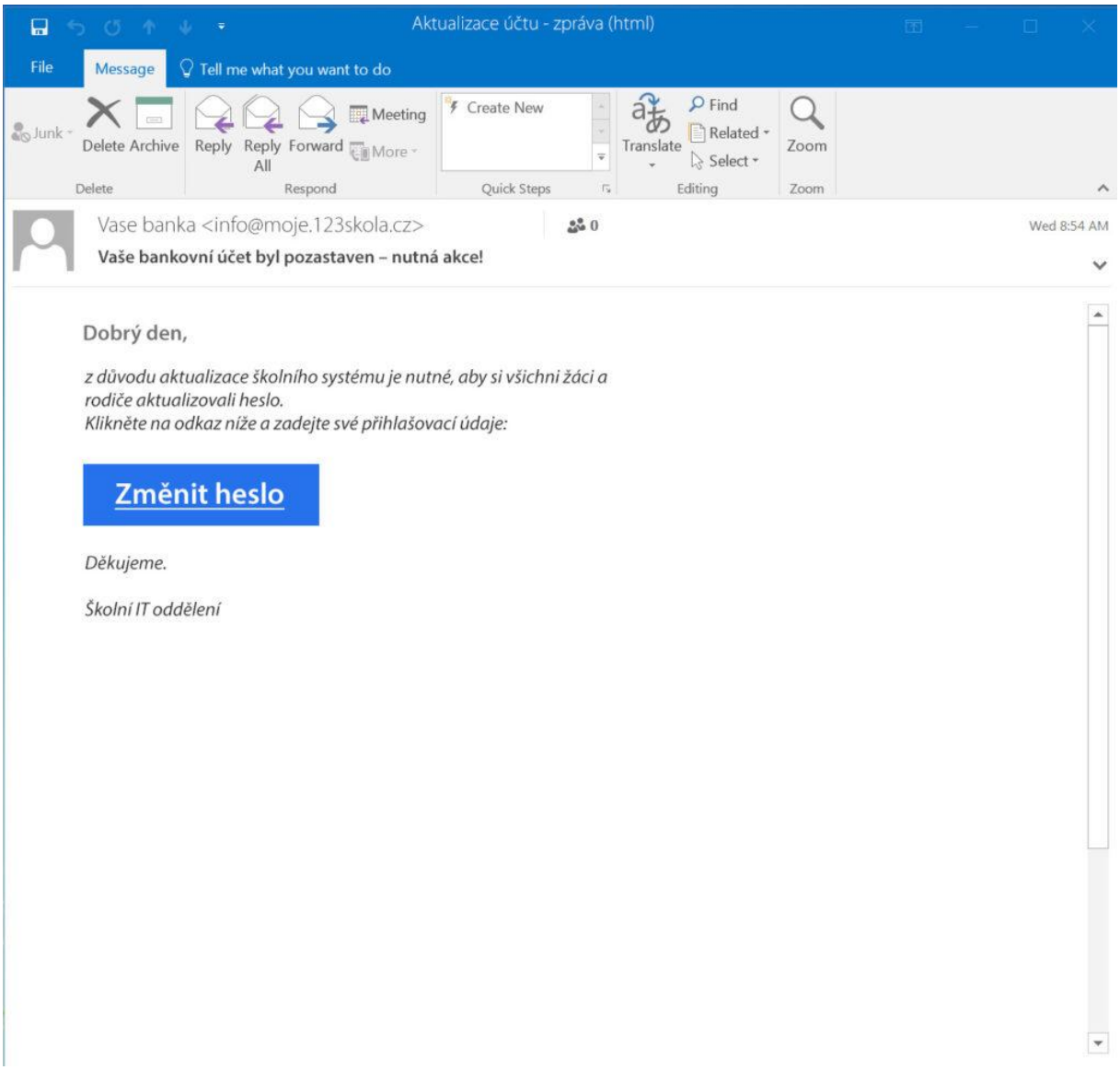
Příklady podvodných e-mailů (phishing)

Phishing je podvodná technika, při níž útočník rozesílá falešné e-maily, které vypadají jako od důvěryhodných institucí. Jejich cílem je přimět příjemce, aby poskytl citlivé informace (např. přihlašovací údaje, údaje o platební kartě) nebo klikl na nebezpečný odkaz.

Phishingové e-maily často napodobují vizuální styl známých značek (např. bank, e-shopů nebo veřejných služeb) a snaží se vzbudit dojem naléhavé situace. Působí profesionálně, ale mohou mít drobné chyby nebo neobvyklé odkazy. Podívejte se na nejčastější typy phishingových zpráv a naučte se je rozpoznat včas.



KYBERCHVÍLE
DIGITÁLNÍM SVĚTEM SPOLEČNĚ



Příklady podvodných telefonátů (vishing)

Vishing (zkratka z „voice phishing“) je podvodná technika, při které se útočník snaží telefonickým hovorem vylákat citlivé informace, jako jsou hesla, údaje o platebních kartách nebo přístup do internetového bankovnictví. Vydává se například za bankéře, zaměstnance technické podpory nebo policistu.

Útočník může volat s falešným důvodem – třeba že došlo k podezřelé aktivitě na účtu, že je nutné ověřit údaje nebo vyřešit „bezpečnostní incident“. Používá přitom zastrašování nebo vytváří pocit naléhavosti. Někdy umí i zfalšovat číslo volajícího, aby to vypadalo, že jde skutečně o banku nebo úřad. Níže uvádíme typické situace, ve kterých vishing útočí – a jak je rozpoznat.