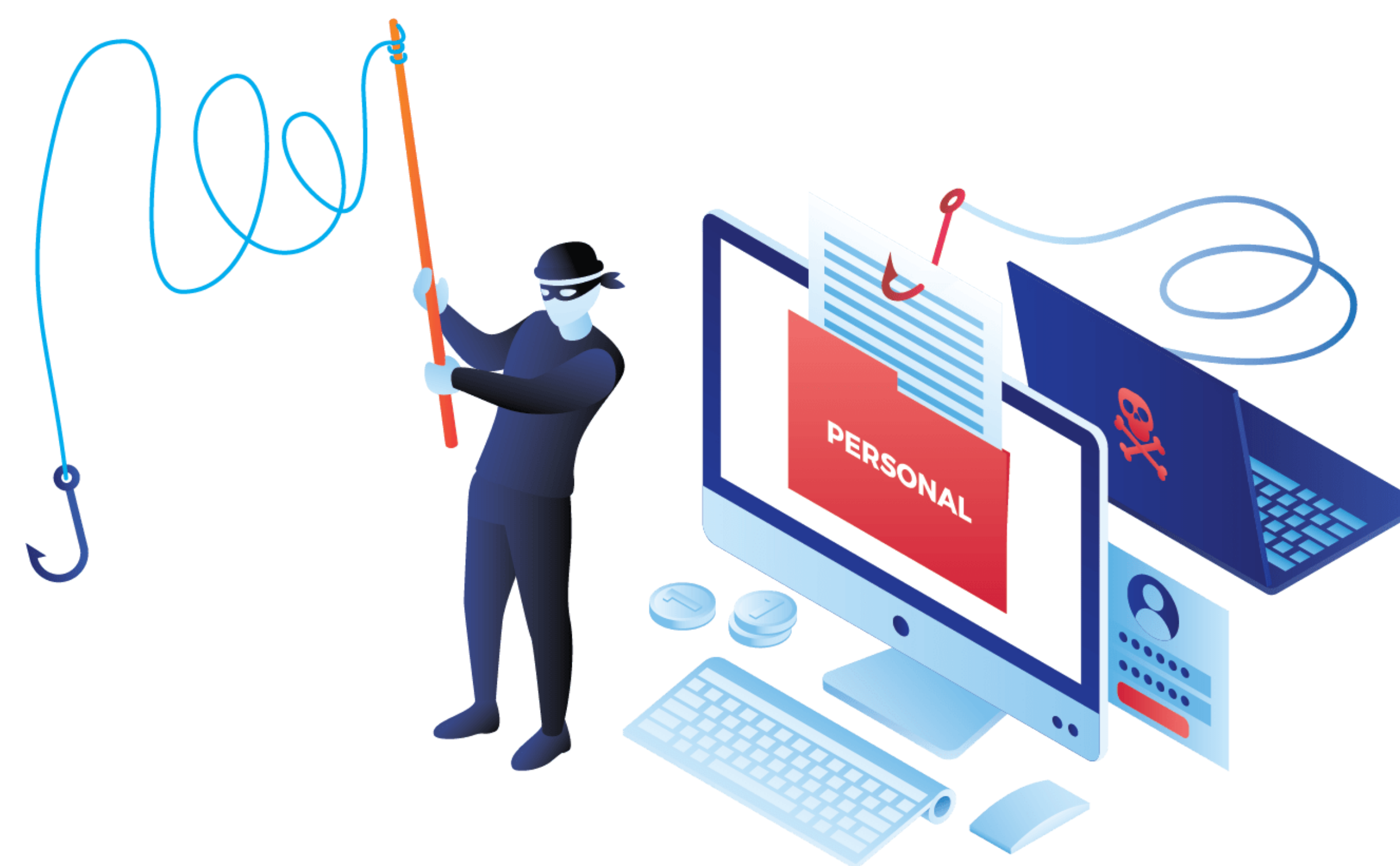


PHISHINGOVÝ TEST

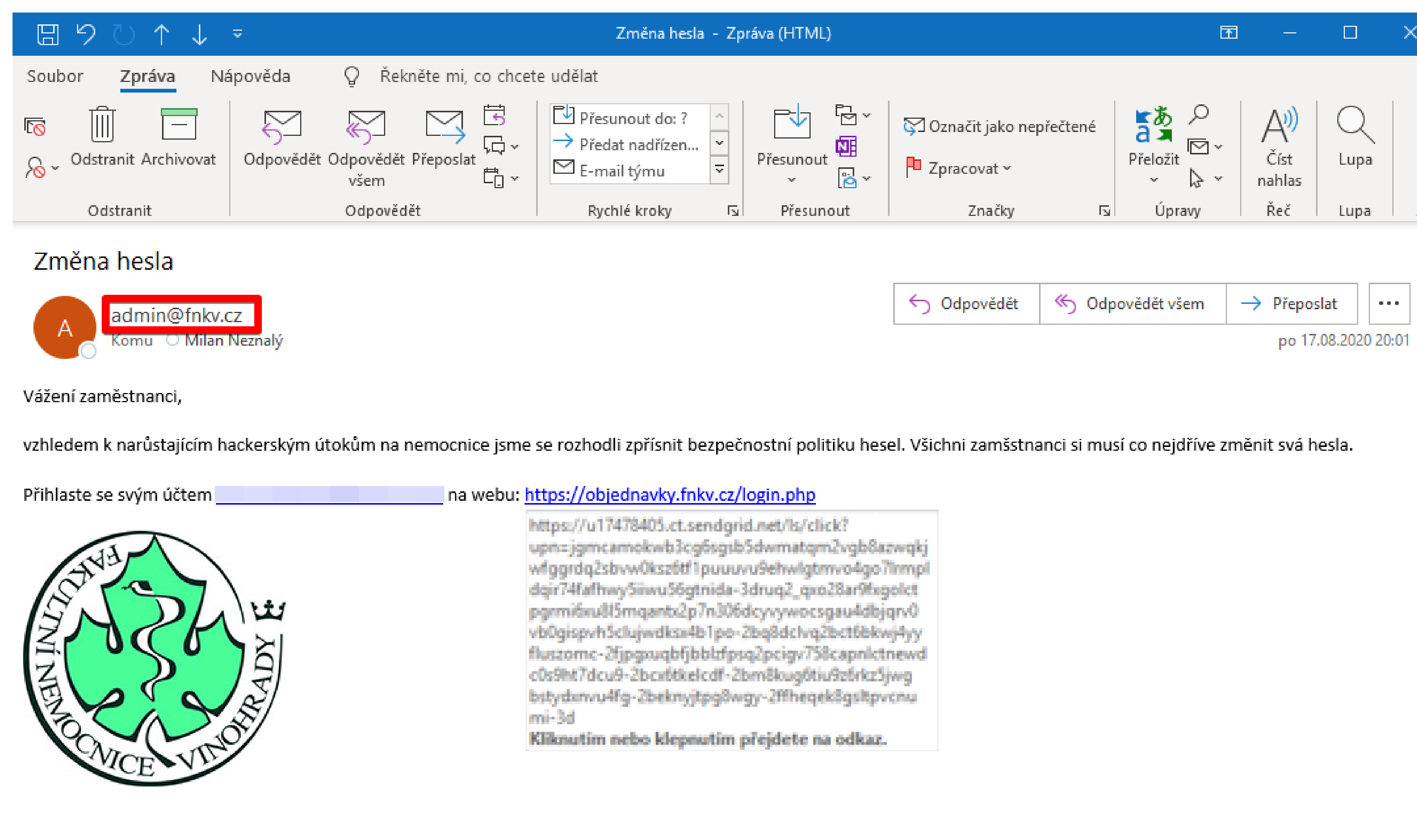
Phishingový test spočívá v tom, že pošleme várku podvržených e-mailových zpráv tak, aby vypadaly, že jsou to zprávy korektní. Reakce uživatelů na doručenou podvrženou zprávu pak shrneme do výsledného hodnocení, které obsahuje přehledné statistiky i seznam doporučení, co vylepšit.

Phishing je jeden z nejčastějších vektorů průniku do firem. Díky phishingovému testu získáte představu o tom, jak by Vaše organizace reagovala v případě, že by se na ni zaměřili hackeři.

Phishingový test je i skvělý podklad pro vzdělávání zaměstnanců. Lidé po tom, co jim oznámíte výsledky testů, reagují obvykle dosti překvapeně a mají mnohem větší zájem se o bezpečnosti dozvědět více.

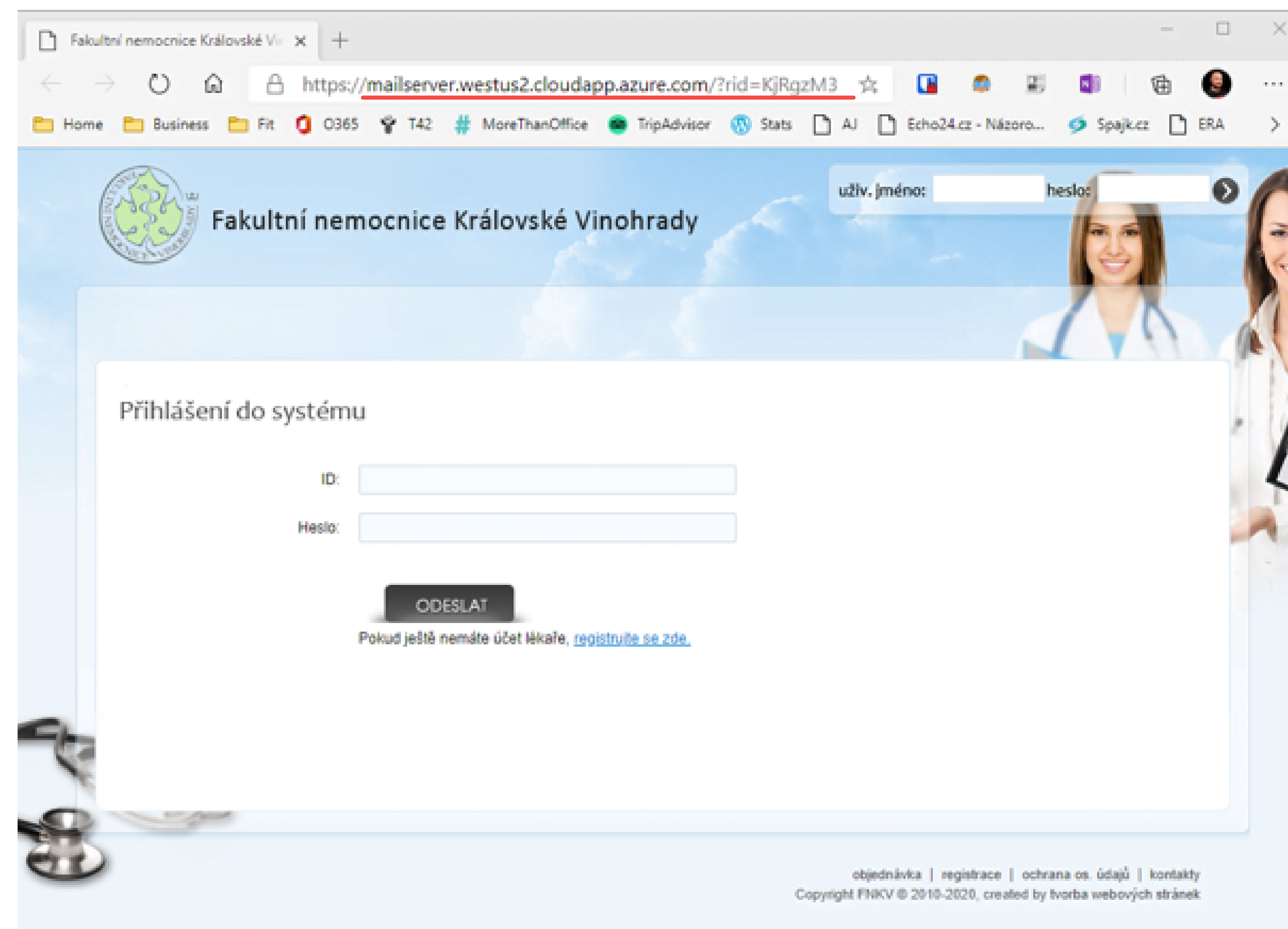


Nejprve pošleme uživateli e-mail. Záleží na domluvě se zákazníkem, jak moc náročné bude jeho odhalení – od běžného phishingu s nabídkou slevy na nákupy až po spear phishing (cílený phishing), který bude bez chyb a k nerozeznání od originálu.



Je dobré nechat v e-mailu vždy nějaké vodítko, například překlep. Uživatel si má také možnost všimnout si linku, který odkazuje na zcela jinou adresu.

Uživatel je po prokliku přesměrován na podvodnou stránku pro přihlášení do systému. Stránka běží na https a krom jiné url je zcela identická. Uživatel se pokusí přihlásit.



K přihlášení nedojde, zadané údaje mohou být zaslány do phishingového systému (nemusí) a uživatel je přesměrován na regulární přihlašovací stránku organizace – zde se již normálně přihlásí a pokračuje v práci. Uživatel si obvykle ani nevšimne, že zadal údaje do podvodné stránky, to že se napoprvé nepřihlásí přičítá obvykle špatně zadanému heslu, nebo chybě stránky.

Pokud nebude phishingový test na Vaše přání anonymní, předáme Vám veškerá naměřená data pro možnosti budoucí analýzy či porovnání v případě opakování testu. Samozřejmostí je smlouva o mlčenlivosti (NDA).

Pro každé oddělení Vaší společnosti můžeme vytvořit zvláštní e-mail tak, aby byla podvodná kampaň co nejdůvěryhodnější. Nebo poslat stejný e-mail všem. Na detailech se s Vámi dohodneme a zvolíme optimální postup.

Měříme poměr mezi doručením, otevřením i proklikem z e-mailu, zaměříme se i na nejobvyklejší časy otevření podvodného e-mailu. Kampaně můžeme poslat najednou, nebo ve vlnách rozložených do delšího časového období.

Pokud nebude i Vaše interní IT předmětem testu, můžeme s ním spolupracovat a vyladit kampaň k dokonalosti a na míru Vaší organizaci.

Součástí testu prověříme i OSINT. Prozkoumáme veřejně dostupné, i když ne na první pohled viditelné informace o Vaší společnosti a Vašich zaměstnancích. Nepoužívají náhodou firemní e-mail pro soukromé účely?

Výsledky shrneme do výsledného hodnocení, které obsahuje přehledné statistiky i seznam doporučení, co vylepšit. Měříme jak byla kampaň úspěšná – zjistíme kolik uživatelů zprávu otevřelo, kolik jich kliknulo na podvodný odkaz, v kolik hodin a na kterém zařízení. Také uvidíme, kolik zaměstnanců se dokonce přihlásilo do falešného portálu, který pro ten účel připravíme. Prezентaci managementu provedeme my, nebo Vaše IT oddělení, dle Vašeho přání.

