Hrozba / Atribut	NÍZKÁ	STŘEDNÍ	VYSOKÁ	KRITICKÁ
Obsah e-mailu	Útočník generuje takový obsah, který by měl zaujmout co největší počet příjemců, a tudíž jeho obsah neodpovídá tomu, co daná organizace nebo zaměstnanec řeší ve svém osobním nebo pracovním životě.	Útočník zohledňuje to, co by daná osoba mohla ve svém soukromém nebo pracovním životě řešit a v případě zaměstnance pak zohledňuje prostředí organizace.	Útočník využívá informací o zamýšlených příjemcích emailu získaných s pomocí OSINT sběru informací.	Útočník ovládnul e-mailový účet odesílatele a z něj odpovídá na e-mail, příjemci, takže ten dostává odpověď, kterou očekává.
Textu e-mailu	Text e-mailu je v jiném jazyce nebo již na první pohled obsahuje značné množství gramatických a stylistických chyb a je zřejmé, že se jedná o strojový překlad. Ve větách si můžeme všimnout špatného slovosledu, skloňování, časování, a nevhodných slovních spojení a obratů.	Text e-mailu obsahuje poměrně dost gramatických a stylistických chyb, a je zřejmé, že se jedná o strojový překlad. Některé věty jsou téměř bez chyb, jiné ale naopak chyby obsahují. Je zřejmé, že text je poskládán z různých originálních textů.	Text e-mailu neobsahuje na první pohled žádné gramatické a stylistické chyby, anebo se jedná o takové chyby, se kterými se naprosto běžně setkáváme i v oficiálních e-mailech. Je zřejmé, že zde již bylo využito služeb někoho, kdo ovládá daný jazyk.	Text e-mailu je prost gramatických a stylistických chyb a je evidentní, že ho psal rodilý mluvčí znalý navíc i prostředí, ve kterém se příjemce e-mailu pohybuje. S takovými e-maily se setkáváme především u spear phishing a whaling kampaní.
Odesílatel e-mailu	E-mail přichází z naprosto nesmyslné automatem generované adresy, a na první pohled je zřejmé, že žádná organizace by takovou adresu nikdy nepoužila.	E-mail přichází ze zcela jiné domény, než kterou používá organizace, za kterou se odesílatel vydává. Je však změněna hodnota v poli FROM na adresu, kterou používá organizace, za kterou se odesílatel vydává.	E-mail přichází z domény ne nepodobné doméně, kterou používá organizace, za kterou se odesílatel vydává. Též je změněna hodnota v poli FROM na adresu, kterou používá organizace, za kterou se odesílatel vydává.	E-mail skutečně přichází z domény důvěryhodné instituce nebo od někoho, koho příjemce e-mailu dobře zná, a kdo byl již kompromitován.
Oslovení adresáta	Oslovení adresáta v úvodu e-mailu je neosobní a často navíc i s chybějící interpunkcí. (např. Dobry den)	Oslovení adresáta v úvodu e-mailu je neosobní, ale bez chyby. (např. Dobrý den)	Adresát je osloven jménem, ale s chybami (např. (Dobry den pane Novak, pokud se příjemce e-mailu jmenuje Novák)	Adresát je správně osloven jménem (např. Dobrý den, pane Nováku, pokud se příjemce e-mailu jmenuje Novák)
Kontaktní údaje	Kontaktní údaje v závěru e-mailu nejsou uvedeny žádné nebo nekorespondují se jménem uvedeným v poli FROM, a kdo vystupuje jako odesílatel e-mailu.	Kontaktní údaje v závěru e-mailu jsou smyšlené, nicméně korespondují se jménem, které je uvedeno v poli FROM, a kdo vystupuje jako odesílatel e-mailu.	Kontaktní údaje v závěru e-mailu jsou pravdivé, adresát se dovolá do skutečné organizace, kde má šanci zjistit, jak se věci mají.	Kontaktní údaje v závěru e-mailu jsou pravdivé až na telefonní číslo, kdy se adresát dovolá na tel. číslo podvodníka, kde je mu potvrzeno, že e-mail je nezávadný.
Odkaz v e-mailu	Na první pohled je zřejmé, že odkaz v e-mailu vede na doménu, kterou organizace, za kterou se odesílatel vydává, nepoužívá.	Po najetí myší na odkaz v e-mailu se zobrazuje jiný odkaz a to na doménu, kterou organizace, za kterou se odesílatel vydává, nepoužívá.	Po najetí myší na odkaz v e-mailu se zobrazuje odkaz na podobnou doménu, která může být i chráněna certifikátem.	Po najetí myší na odkaz v e-mailu se zobrazuje odkaz na pravou doménu chráněnou certifikátem.
Formulář v e-mailu	E-mail je rozesílán ve formátu HTML s formulářem požadující zadání citlivých údajů, a neobsahuje žádné grafické prvky a nesnaží se ani napodobit grafický styl organizace, za kterou se útočník vydává.	E-mail je rozesílán ve formátu HTML s formulářem požadující zadání citlivých údajů, a používá podobných barev a obrázků jako organizace, za kterou se odesílatel vydává.	E-mail je rozesílán ve formátu HTML s formulářem požadující zadání citlivých údajů, a používá stejných barev a obrázků jako organizace, za kterou se odesílatel vydává, ale ty jsou stahovány z domény útočníka.	E-mail je rozesílán ve formátu HTML s formulářem požadující zadání citlivých údajů, a používá stejných barev a obrázků jako organizace, za kterou se odesílatel vydává a z té jsou i stahovány.
Příloha e-mailu	Přílohou e-mailu je archiv obsahující spustitelný soubor a odesílatel se to ani nesnaží nijak skrýt (např. exe, scr)	Přílohou e-mailu je archiv obsahující spustitelný soubor a odesílatel se to snaží zamaskovat dvojitou příponou (např. jpg.exe rtf.exe, pdf.exe) a zneužít skutečnosti, že ve Windows se nemusí zobrazovat známé přípony.	Přílohou e-mailu je archiv obsahující spustitelný soubor, který se reprezentuje ikonou dokumentu např. PDF nebo DOC a případně se i maskuje dvojitou příponou.	Přílohou není spustitelný soubor, ale např. PDF nebo DOC, který obsahuje škodlivý kód a zneužívá zranitelnosti (nultého dne) v přidružené aplikaci.

Zdroj: cleverandsmart.cz **Verze 1.2**