GOMEZ
the finest premium brands

HROZBY SPOJENÉ S POUŽÍVÁNÍM ELEKTRONICKÝCH SLUŽEB

Osoby, které využívají elektronické služby, se mohou setkat s těmito hrozbami:

Spam	Příjem nevyžádaných reklamních (komerčních) informací elektronickou cestou.
Malware	Software, který je schopný po spuštění infikovat soubory aniž by si toho uživatel všiml. Mají různé efekty a účinky, zabírají paměť RAM, CPU a prostor na pevném disku.
Worm	Software, který se může sám kopírovat. Emailový červ je ničivý útok proti sítím, který shromažďuje internetové adresy a následně na ně posílá stovky infikovaných emailů s neviditelnou přílohou.
Spyware	Software, který špehuje uživatele na internetu, instaluje se bez souhlasu, vědomí a znalosti uživatele.
Škodlivý software	Nechtěny nebo „škodlivý" software, který běží na pozadí bez vědomí uživatele, např.: trojan, wabbit, rootkit, keylogger, backdoor, exploit.
Cracking/phishing („zloděj hesel")	Snaží se prolomit bezpečnost (cracking) a získat osobní údaje za účelem krádeže totožnosti. Zasílá falešné emaily, které jsou nerozpoznatelné od pravých.
Sniffing	Neoprávněný odposlech, který spočívá v používání programu sniffer – program, jehož úkolem je zachytit a analyzovat data v síti.
Kryptoanalýza	Hledání slabých míst v kryptografickém systému, které by umožnily jeho prolomení nebo obejití.
Používání nelegálních zařízení	Zavedení třetí osobu do telekomunikačního systému nelegální zařízení, které poskytuje neautorizovaný přístup k chráněným službám.

Aby se předešlo výše zmíněným hrozbám, měl by Zákazník, dřív než svoje zařízení připojí k internetu, mít nainstalovaný aktuální antivirový program a zapnutou firewall bránu. Zákazník by měl také chránit svojí emailovou schránku antivirovým programem, který vyhledává viry v emailech a kontroluje příchozí soubory před jejich otevřením.