GOMEZ
the finest premium brands

NEBEZPEČENSTVO SPOJENÉ S VYUŽÍVANÍM SLUŽIEB POSKYTOVANÝCH ELEKTRONICKOU CESTOU

Osoby využívajúce služby poskytované elektronickou cestou môžu byť vystavené nižšie uvedeným nebezpečenstvám:

Spam	Doručenie neobjednanej reklamnej (obchodnej) informácie elektronickou cestou.
Malware	Softvér, ktorý je schopný po spustení nakaziť súbory a ďalej sa rozširovať bez toho, aby o ňom užívateľvedel. Predmetné softvéry majú rôzne účinky, napádajú pamäť RAM, CPU a pevný disk.
Worm	Softvér schopný samorozmnožovania. E-mail worm útočí na sieť tak, že po zozbieraní vštkých e-mailových adries, ktoré sa nachádzajú v programe obsluhujúcom poštu rozpošle stovky e-mailov obsahujúcich červa v neviditeľnej prílohe.
Spyware	Samoinštalačný softvér sledujúci činnosť užívateľa na internete bez jeho súhlasu a kontroly.
Zlomyseľný softvér	Nežiadúce alebo „zlomyseľné" softvéry, vykonávajú činnosti ako napr.: trójske kone, wabbit, rootkit, keylogger, backdoor, exploit.
Cracking/phishing („lovenie hesiel")	Činnosti, ktorých cieľom je odstánenie ochranných mechanizmov (cracking) a získanie konkrétnych informácií, o.i. krádež identity, prostredníctvom zasielania falošných elektronických správ, ktoré vyzerajú autenticky.
Sniffing	Nelegálne odpočúvanie, využívajúce sniffer – počítačový program, ktorého úlohou je uchovávanie a analyzovanie údajov umiestnených v sieti.
Kryptoanalýza	Vyhľadávanie slabín v kryptografickom systéme, ktoré umožňuje jeho rozbitie alebo obídenie.
Používanie nelegálnych zariadení	Zavedenie nelegálnych zariadení do teleinformačného a/alebo telekomunikačného sysému inými osobami, ktoré umožňujú neoprávnený prístup k službám podliehajúcim ochrane

Zabezpečenie svojho zariadenia prepojeného s internetovou sieťou pred vyššie uvedeným nebezpečenstvom prostredníctvom aktuálneho antivírusového programu a firewallu je na plnú zodpovednosť Zákazníka. Okrem toho Zákazník zodpovedá aj za zabezpečenie svojej elektornickej pošty v programe, ktorý dokáže detekovať prítomnosť vírusov v e-mailových správach a kontrolovať importované údaje pred ich otvorením (spustením) pomocou modulu skenujúceho súbor antivírusového programu. Gomez nenesie v žiadnom ohľade zodpovednosť za akákoľvek škody spôsobené vyššie uvedeným nebezpečenstvom Zákazníkovi.