

SCROLLUJ

Online hry nepřináší jen zábavu, ale i rizika.

TAK O CO TADY JDE?

Vše, co byste měli vědět o hrách!

KONZOLOVÉ HRY

MOBILNÍ HRY

POČÍTAČOVÉ HRY

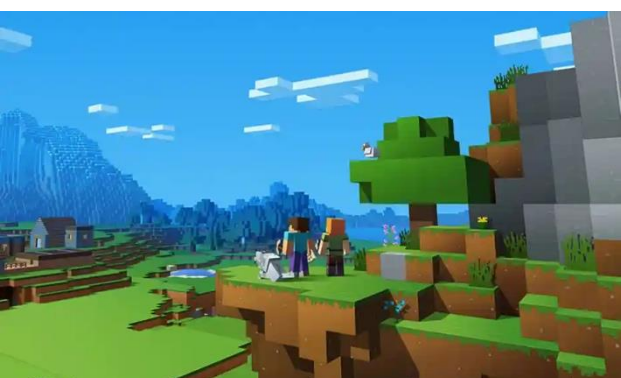
WEBOVÉ HRY

KYBERŠIKANA

PODVODNÍCI

PREDÁTOŘI

OBSAH



Co to jsou online hry?	2
Kde všude se dají hrát online hry?	3
Konzolové hry	3
Mobilní hry	3
Webové hry	4
Počítačové hry	4
Čeho se obávat?	5
Podvodníci	5
Predátoři	6
Mikrotransakce	7
Malware	8
Falešné programy	9
Kyberšikana	10
Závěr	12

TAK O CO TADY JDE?

VŠE, CO BYSTE MĚLI VĚDĚT

Současný svět představuje nepřeberné množství možností, jak trávit volný čas. Nabízí řadu odvětví, v nichž člověk hledá smysl svého vyžití a uspokojení, navzájem se prolínají a střídají. Mohou být spjaté s přírodou, se sportem, s uměním, s kulturou, ale i s moderními technologiemi.

Ty se rok od roku zdokonalují a pronikají do trávení volného času člověka už od svého úplného počátku. Hraní her se stále více stává velmi oblíbenou aktivitou, a to jak u mladší, tak mezi starší generací. Online hry se dají hrát už na každé platformě, jako je třeba mobilní telefon, počítač nebo konzole.

Najdeme mezi nimi velikou škálu variací. Od her sportovních, k hrám, které jsou založeny na tom, že plníte úkoly a sbíráte užitečné suroviny, k

simulátorům, a tak podobně. Online hry umožňují hráči spojit se s ostatními, hlavně prostřednictvím dnes už tak rozšířeného internetu a hrát s nimi nebo proti nim. Hrát můžete s kamarády, rodinou nebo dokonce s někým, kdo je na druhé straně Země. Zjednodušeně online hry spojují obrovská kvanta lidí. S tímto bohužel přicházejí i rizika a nebezpečí, kterými Vás tento časopis provede.

Počítače i počítačové hry jsou a budou součástí budoucnosti nejen nás, ale i našich dětí. Jejich rozvoj a zdokonalování, pro naši lidskou povahu, nezastavíme a naopak se je budeme snažit zlepšovat a vyvíjet. Proto bychom měli včas upřít svou pozornost na to, jak vlastně působí na naše zdraví, chování, vztahy a celou společnost.

Kde všude se dají hrát online hry?

Existuje několik způsobů, jak si uživatelé mohou online hry zahrát. Nejprve hráč si musí nějakou hru najít, třeba na internetovém vyhledávači. Je zde řádka her, které jsou zadarmo, ale také hry, které jsou za nemalý poplatek. Dále hráč potřebuje platformu, jako je mobilní telefon, počítač nebo konzole, jako je například Play Station, Xbox nebo Wii.

Mobilní hry

Mobilní hry mohou být zdarma nebo zpoplatněné. Můžete si je stáhnout prostřednictvím aplikace, jako je Google Play nebo Apple

Tam s mobilními hrami mohou být spojeny i mikrotransakce, protože v některých hrách, a to i v těch bezplatných, je možné zakoupit dodatečný obsah, například různé herní měny, postavičky a tak dále. Nicméně, tyto funkce lze deaktivovat, a to buď prostřednictvím nastavení v aplikaci, nebo prostřednictvím nastavení účtu Vašeho zařízení v obchodě.



Konzolové hry

Tyto hry se hrají nejčastěji doma. Nejčastěji na televizi. Konzole jsou schopné se připojit k internetu prostřednictvím domácí Wi-Fi sítě, stejně jako jiná zařízení. To uživatelům umožňuje, nakupovat a stahovat hry, kupovat další obsah do her, jako jsou další úrovně, postavy, funkce a tak dále. U konzolí je typické, že k hraní online může být vyžadováno předplatné. Hlavní výrobci konzolí je Nintendo, Sony a Microsoft.

Webové hry

Některé hry jsou přístupné prostřednictvím unikátních webových stránek, na kterých jsou umístěny stovky různých her. Mnohé z těchto her jsou zdarma online, i když některé mohou být placené. Tyto stránky se staly velmi populárními mezi mnoha mladými lidmi, protože se na nich, často nabízí tvůrčí prvek, který uživateli umožňuje vytvářet si vlastní hry.



Počítačové hry

Tyto hry se hrají na počítači. Je k dispozici také velké množství bezplatných her, které jsou od určitého bodu placené, buď jednorázově, nebo prostřednictvím měsíčního předplatné. Spousta počítačových her dnes využívá internet a s tím vzniká mnoho her typu MMO (Massively Multiplayer Online), ve kterých je spousta hráčů ve velkém virtuálním světě, kde hráči společně komunikují a spolupracují. Nebo MOBA (Multiplayer online battle arena), což je žánr hry, v němž se proti sobě v jedné aréně utkávají dva týmy složené z více hráčů. A další.



Čeho se obávat?

Podvodníci

Online hry jsou v současné době plné mikrotransakcí a power gamingu, podvody se postupem času stávají stále častějšími. Ve hrách, jako je World of Warcraft a Runescape, je nejlepší obsah uzamčen za určitými úrovněmi, takže můžete být v pokušení a zaplatit někomu za posílení svých postav. Budou po vás chtít hesla, protože budou tvrdit, že vám zvýší hráčskou úroveň. Jakkoli to může znít lákavě, je to pro online podvodníky skvělá příležitost, jak se zmocnit vašeho profilu.

Většina případů skončí tím, že váš online herní profil převezme někdo cizí a vy už na něj nebudete mít přístup. Pokud byla k tomuto online profilu připojena kreditní karta, pak ji zločinci mohou použít k nákupu zboží pro sebe. To je však jen jeden příklad hrozby, kterému můžete čelit, pokud jde o hraní online her.

Další takovou metodou, na kterou je třeba si dát pozor, je, když jiní online hráči nabízejí neuvěřitelné nabídky placeného obsahu, který je mnohem levnější, než kolik ve skutečnosti stojí. Věci, jako jsou nové úrovně, kosmetické úpravy postav, které se běžně používají při podvodech. Velké množství her má nyní dodatečné služby, za které je třeba zaplatit, čehož mnoho podvodníků běžně využívá k rychlému výdělku.



Jak se bránit?

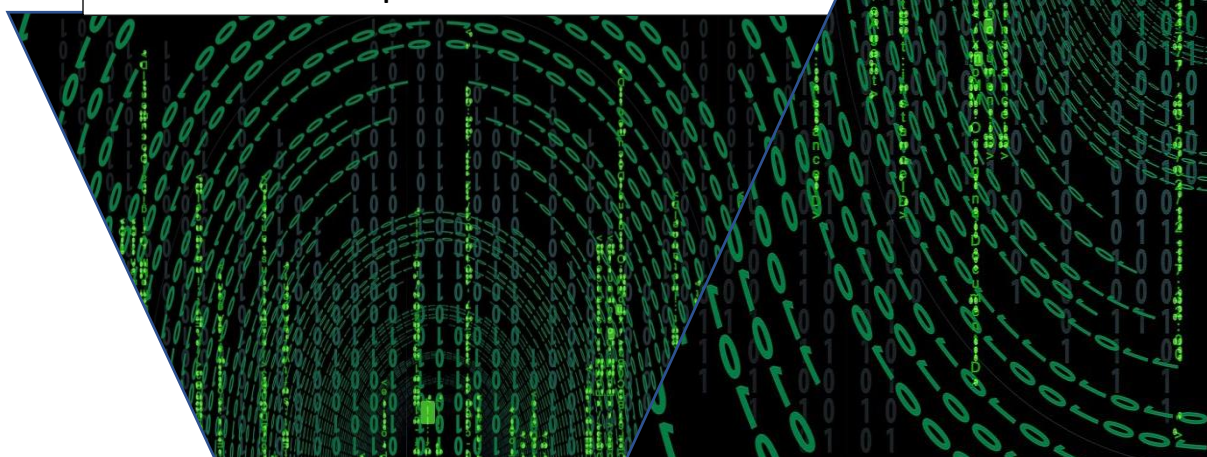
Nikdy a nikomu nesdělovat přihlašovací údaje do aplikací! Tím můžete zabránit ztrátě peněz a ochránit svá systémová data.



Predátoři

Z vyšetřování policie vyplývá, že predátoři vyhledávají oběti všude, kde se s nimi mohou dostat do kontaktu. Online hry jsou jen jednou z mnoha platforem, které predátoři využívají, částečně i kvůli jejich popularitě. Děti mají také tendenci být na internetu důvěřivé a často se přátelí s cizími lidmi jakéhokoli věku nebo pohlaví.

Online hry také poskytují predátorům celkem logické téma pro zahájení konverzace s jejich zamýšlenými oběťmi: jejich společný zájem o hru. Predátoři se mohou vydávat za přátelské dospělé nebo věkově přiměřené vrstevníky, aby navázali vztah s potenciálními oběťmi.



Mikrotransakce

Společnosti vyvíjející videohry používají behaviorální psychologii, aby uživatele silně motivovaly k nákupům ve hře. Tento systém monetizace je tak úspěšný, že se nyní používá ve všech třídách videoher. Studie ukazují, že pravděpodobnost útraty ve hře nemá nic společného s dobou strávenou hraním nebo frekvencí hraní. To znamená, že závislost na videohrách není jediným problémem hráčů a rodičů hráčů. Nicméně každý, kdo hraje videohry, je náchylný k neplánovanému a nadměrnému utrácení ve hrách.

Herní průmysl tyto nákupy ve hře nazývá, jako takzvané mikrotransakce. Protože cena jednoho virtuálního předmětu je často relativně nízká, jsou často tyto předměty sdruženy do cenově výhodnějších balíčků, které hry vyžadují, aby si je hráči kupovali opakovaně, aby mohli ve hře smysluplně postoupit dále.

V některých případech tyto transakce můžeme nazývat Loot Boxy. Nabízejí možnost vyhrát herní předmět různé hodnoty pro hráče. Může se to podobat hazardu, protože při výběru předmětu, který hráč získá, hraje roli štěstí. Z pohledu Komise pro hazardní hry se ve skutečnosti nejedná o hazard, protože vyhrané předměty nemají mimo hru žádnou peněžní hodnotu.

Pokud by to bylo považováno za hazardní hru, nemohla by být prodávána dětem. To je důvod, proč některé země, například Belgie, zakázaly používání loot boxů ve hrách, protože je považují za hazard zaměřený na děti.

Tyto mikrotransakce mohou snadno dosáhnout tisícům, deseti tisícům a přinejmenším v jednom extrémním případě i stotisícům korun. Nejzranitelnější vůči těmto manipulativním monetizačním taktikám jsou děti a dospívající, protože ve své fázi dospívání přirozeně ztrácejí kontrolu, nad těmito podněty.



Malware

Bezpečnost a zabezpečení online nebyly nikdy tak důležité jako dnes. Zabránit škodlivým útokům a napadení počítače malwarem se stalo pro ty, kteří pravidelně používají počítač, nesmírně důležitým každodenním úkolem. To se projevilo zejména v herním světě, kde řadí zloději hesel a pokusy o takzvaný phishing (snaha počítačových podvodníků získat vaše citlivé osobní informace).

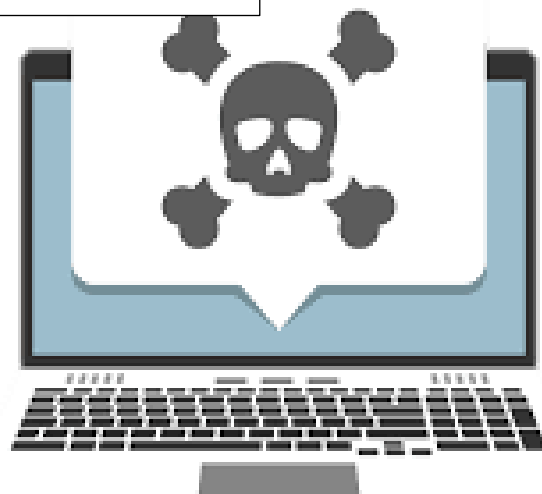
Zloději hesel

Obdrželi jste někdy podezřelou zprávu z účtu, který jste nikdy neviděli, s výzvou ke kliknutí na odkaz na webovou stránku? Pak jste se možná stali cílem útoku zloděje hesel!

Zloději hesel pracují tak, že se vydávají za hráče, kterého znáte, nebo dokonce za jednoho z vývojářů hry a tvrdí, že s vaším účtem nastal problém. Odkaz, který vám pošlou, bude maskován tak, aby vypadal jako jedna z mnoha herních webových stránek, ale bude se jednat o falešnou stránku. Poté vás požádají o zadání údajů o vašem účtu, jako jsou hesla, která používáte. Po zadání údajů se může podvodník snadno nabourat do vašeho profilu.

Jak se bránit?

Nejlepším způsobem, jak tomu zabránit, je vždy zkontrolovat údaje osoby, která vám zprávu poslala, a ujistit se, že jí můžete důvěřovat. Klikání na odkazy se můžete také zcela vyhnout tím, že ručně vyhledáte správné herní stránky, abyste si mohli být jisti, že jde o ty pravé. Předějit tomuto problému můžete, také pomocí nastavení filtru nevyžádaných zpráv, který zabrání zaslání nevyžádaných zpráv a e-mailů.



Falešné programy

Největším způsobem šíření malwaru v herním průmyslu je dnes pravděpodobně používání virů skrytých ve zdrojovém kódu. Ukrytí viru do herních souborů, avšak není jediným způsobem, jak lze pomocí falešného programu nakazit počítač malwarem. Hackeři také nahrávají falešné verze známých programů nebo online her, které obsahují malware, což lze označit jako trojský kůň.

Uživatelé počítačů nebo hráči si tyto produkty nainstalují do svých zařízení, aniž by si uvědomili, že se ve skutečnosti jedná o falešné programy, které hostí malware, jako jsou keyloggery nebo ransomwaery. Po instalaci si nejprve všimnete velkého množství využívaných systémových prostředků, které zpomalují výkon vašeho počítače. To může následně přerůst v krádež hesel a změnu e-mailu na některých účtech.

Jak se bránit?

První a nejlepší ochrannou, jak se bránit, je zajistit aktualizaci antivirového programu (Avast, ESET, atd.). Antivirové programy jsou jednou z nejlepších metod ochrany, ne-li tou nejlepší. Zkontrolujte také, zda všechny programy a aplikace stahované z internetu pocházejí z důvěryhodných stránek.



Kyberšikana

Skutečnost, že internet a sociální média jsou tak snadno dostupné, poskytuje lidem možnost posílat výhrůžky, vydírat a šikanovat ostatní online a přitom sami zůstat v anonymitě. V tomto článku se budeme zabývat tímto novým fenoménem.

Co to je kyberšikana?

Podle mnoha autorů se kyberšikanou rozumí šikana, která zahrnuje využívání internetové platformy při používání chytrých telefonů, počítačů nebo jiných elektronických zařízení k úmyslnému a opakovanému způsobování fyzické a nebo emocionální újmy oběti jednotlivcem nebo skupinou lidí. O kyberšikaně existují některé mylné představy. Třeba, co se týká věku, ve kterém ke kyberšikaně dochází. Můžeme mluvit o kyberšikaně, kyberobtěžování nebo kyberstalkingu. Rozdíl mezi těmito pojmy spočívá v tom, že ke kyberšikaně dochází mezi nezletilými, zatímco v případě, že se jedná o dospělého, lze toto chování označit jako kyberobtěžování nebo kyberstalking.



Rozšíření a globalizace kyberšikany

V minulosti museli lidé fyzicky doručit zprávu někomu ve vzdálené části světa. Dnes se téměř vše děje stisknutím tlačítka. Svět se mění; už není tak velký a rozlehlý jako kdysi. Globalizace díky technologickému pokroku svět zmenšila a více propojila. Vedla k vytvoření nového světa, v němž je internet využíván v dobrém i ve zlém.

Internet, který umožňuje všechny druhy komunikace a udržuje svět ve spojení, je jednou z nejdůležitějších hnacích sil globalizace. Pozitivním aspektem je, že internetovou infrastrukturu lze využít mnoha způsoby. Například k online nakupování, hraní online her nebo spojení se s příbuzným na druhé straně zeměkoule. Vše, co lze využít pozitivně, lze však využít i negativně. Jednou z negativních stránek digitálního světa a jeho anonymní dostupnosti je, že lidé

Kyberšikana versus tradiční šikana

Podle výzkumu Kowalského, Limbera a Agatsona (v roce 2012) má kyberšikana s tradiční šikanou společné tři základní charakteristické rysy. Prvním je, že se jedná o agresivní chování. Za druhé se toto chování opakuje. Poslední charakteristikou je, že oběť je slabší než osoba, kterou je šikanován, to u kyberšikany je hlavně z psychologického hlediska. Šikana, je však při použití internetových prostředků do jisté míry jiná než při interakci tváří v tvář. Některé teorie naznačují, že kyberšikana je mnohem horší, než se většina lidí domnívá.

Kyberšikana v online hrách

Anonymita hráčů a používání avatarů umožňuje uživatelům vytvářet alter-ega nebo fiktivní verze sebe sama, což je součástí zábavy při hraní. Zároveň však uživatelům umožňuje obtěžovat, šikanovat a někdy i hromadně napadat ostatní hráče. Pokud jsou hráči anonymní, může být obtížné je pohnat k odpovědnosti, když šikanují ostatní a používají hru jako nástroj obtěžování. Někteří hráči mohou hru používat jako prostředek k obtěžování ostatních nebo k získávání jejich osobních údajů, jako jsou uživatelská jména a hesla. Mohou dokonce zpřístupnit osobní údaje ostatních online prostřednictvím taktiky zvané "doxing". Doxing může ohrozit nejen informace o dítěti, ale i o jeho rodičích, a může z nich učinit terče šikany a obtěžování.

Hráči často využívají online herní komunity a sociální média k tomu, aby se spojili s ostatními hráči, učili se tipy a triky, sdíleli strategie, vytvářeli týmy/gildy a navazovali kontakty při hraní nebo sledování hraní ostatních. Tyto typy online komunit jsou také místem, kde se kyberzločinci mohou snažit způsobit škodu – například zveřejněním odkazů, které se zdají být spojené s hrou, ale ve skutečnosti se jedná o počítačové viry nebo malware (software určený k narušení, poškození nebo získání přístupu k počítači), nebo kde se predátoři mohou snažit získat přístup k dětem.



Závěr

Dnešní online hry jsou bohužel plné bezpečnostních rizik, ale ta, o kterých jsme se dnes zmínili, jsou jen některá, která vám hrozí od ostatních hráčů a pochybných webových stránek. Nejlepší online ochranou je instalace antivirového systému, který zabrání tomu, abyste se stali obětí ztráty dat. Součástí přitažlivosti online her je svoboda hrát kdykoli s velkým počtem uživatelů, ale to také znamená, že mohou představovat hrozbu pro řadu obětí.

Velké nebezpečí se také skrývá za používáním sociálních sítí. V dnešní době internetu a virtuálního světa je kontakt s druhým člověkem neosobní, nevidíte mu do tváře, a proto si nikdy nemůžete být jisti, kdo se na druhém konci opravdu skrývá. Kdokoliv si může založit profil s falešným jménem, fotografií a údaji a vytvořit si tak zcela novou identitu. Nejvíce ohroženou skupinou, která by se mohla stát obětí podvodníka nebo násilníka jsou děti, především pak dívky ve věku od 12 do 15 let.