

Projekt IT-Sicherheit und Social Media-Plattformen – Grenzüberschreitende Prävention – Sicher im Internet

Projekt IT-bezpečnost a sociální média – Přeshraniční prevence – Bezpečnost na internetu

**Projekt - Nr. 3-17-7018
Číslo projektu**



Inhalt

Definitionen	3
Definice	3
Sicherheit und Passwörter	4
Bezpečnost, bezpečnostní heslo:	5
Malware – Schutz vor Viren	9
Viry – Prevence	10
Verschlüsselt/ Sicher chatten	11
Šifrování – bezpečné chatování:	12
Kde a jak se kyberšikana objevuje:	13
Wo und wie Cybermobbing tritt auf:	15
Dobré rady, co udělat, pokud na nás někdo útočí přes sociální sítě: .	18
Gute Ratschläge, was zu tun ist bei einem Angriff über soziale Netzwerke:	18
KDE HLEDAT POMOC nebo KAM SE OBRÁTIT?	19
.....	22
Kyberšikana	22
Gefährliche Internettrends	24
Auswertung Umfrage Augustusburg	25
Graf kyberšikana:	28
Teilnehmer	31

Definitionen

Firewall: soll verhindern das Unbefugte auf den privaten PC oder auf von Unternehmen erstellte Systeme zugreifen können.



Live CD:

- ↳ ein Direktstartsystem;
- ↳ kann ohne Installation und Beeinflussung des Inhaltes auf einer im System vorhandenen Festplatte gestartet werden.

Malware (Computerprogramm):

- ↳ aus dem eng.: Mal – malicious (böartig); Ware – Software;
- ↳ führt unerwünschte bzw. schädigende Handlungen auf dem Computer aus.

Mobbing: „Psychoterror“ mit dem Ziel das Opfer zu schikanieren, zu quälen und seelisch zu verletzen.

Definice

Brána firewall: nepodporované systémy založené v počítačích nebo systémy vytvořené firmou, kde se mohou naše počítače nakazit.

Live CD:

- ↳ systém přímého startu;
- ↳ může být použit k instalaci a používání instalačních systémů v budoucnosti.

Malware: (počítačový program):

- ↳ z úzkého: Mal (zlý); Ware – software;
- ↳ provádí nežádoucí popř. škodlivé akce v počítači.

Mobbing: "Psychoterror" s cílem obtěžovat, mučit a psychicky týrat oběť.

Sicherheit und Passwörter

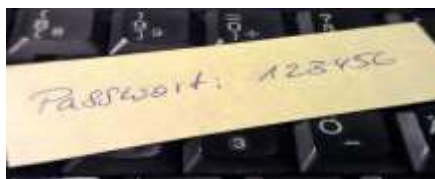


- Wenn du dich auf Social Media Plattformen anmeldest musst du dein Alter angeben und die Nutzungsbedingungen gelesen und verstanden haben.
- Sei vorsichtig, wen du als Freunde (z.B.: Facebook) akzeptierst.
- Wenn du mit jemandem fremden über das Internet chattest, dann verraten ihm/ihr keine persönlichen Daten (Adresse, Passwörter, etc.)
- Rede nicht mit fremden Personen über deine Probleme, da du nicht weißt, was diese mit diesen Infos anstellen.
- Sende keine Fotos, die dich in deinem alltäglichen Umfeld zeigen.
- Gehe nicht alleine mit fremden Personen aus, außer du nimmst eine zweite Person mit oder du hast jemandem davon erzählt, mit dem du in Kontakt bleibst, oder trefft euch nur an einem Ort
- wo viele andere Menschen sind!
- Mobbe nicht!



Passwortsicherheit

- Ändere alle 3 Monate dein Passwort! Es sei denn, du hast den Verdacht, dass eine andere Person dein Passwort weiß, dann ändere es sofort.
- Ein wirklich sicheres Passwort sollte mindestens 8 Zeichen (Buchstaben, Zahlen, Sonderzeichen etc.) haben. Verwende aber keine Persönlichen Daten als Passwort! (Adresse, Name, Geburtsdatum,...)
- Neumodische Passwörter (Augen- und Fingerabdruckscan) sind nicht so sicher wie eine Pin oder ein Passwort.
- Gib dein Passwort niemals preis!
- Speichere niemals ein Passwort im Internet für irgendeine Webseite!!



Bezpečnost, bezpečnostní heslo:

Chování na sociálních sítích:

- Vytváříte-li si sociální sítě, měli byste na to mít věk a rozum (při přihlášení je nutné udat svůj věk a je nutné akceptovat povinné podmínky).
- Bud'te opatrní, koho přijímáte do okruhu svých přátel.
- Když si píšete s cizí osobou, nesděľujte své osobní údaje, které by mohli být zneužity (adresa, hesla...)!
- Nemluvte o svých problémech s cizí osobou!
- Neposíľajte osobní fotografie a podobné věci!
- Nechoďte na schůzku s neznámou osobou:
 - ↳ řekněte někomu o schůzce;
 - ↳ na první schůzku běžte s doprovodem (kamarád...);
 - ↳ setkání musí být někde tam, kde je hodně lidí.
- Nebud'te kybernetickým zločincem!



Bezpečnostní heslo:

Každé 3 měsíce si změň heslo:

- ↳ pokud jiná osoba ví vaše heslo, změňte si ho,
- ↳ upravuj si heslo 2-3 krát do roka.

Heslo by mělo obsahovat aspoň 8 znaků:

- ↳ čím delší heslo bude, tím se stává bezpečnější.

Jak vytvořit bezpečné heslo?

- ↳ krok 1: vytvoř si vlastní slovo, které bude obsahovat znaménka (?, !, ., _ :);
- ↳ krok 2: nevytvářej si heslo s osobními údaji (adresa, narozeniny.....)
- ↳ nezveřejňuj ho (nikdy nenechávej své heslo volně zobrazovat, nikdy neukládej své heslo pro různé webové stránky).

Nová metoda: scan prstu nebo oka => méně bezpečná.

Mein Bild, Dein Profil

Vorsicht beim Hochladen!

Facebook richtet durch Gesichtserkennung eigenständig Profile für Nutzer ein, welche auf Bildern zusehen sind jedoch kein Facebook besitzen.

- Betroffene bekommen nichts von den Accounts mit.
- Facebook-Software ermittelt sich die Identität der Personen selbst, durch weitere Informationen wie z.B. Ort, Schule, Freunde.

- ↳ Sämtliche Personen auf deinen Bildern müssen gefragt werden und zustimmen.
- ↳ Wenn nicht, dann müssen diese Menschen unkenntlich gemacht werden oder das Bild darf erst gar nicht hochgeladen werden
- ↳ Man muss damit rechnen, dass sich jedes Bild schnell im ganzen Netz verbreiten kann.

Überlege was man hoch lädt!

- Beispielsweise Einbruchsgefahr während des Urlaubs.



Bildrechte

Facebook darf alle hochgeladenen Bilder kostenlos für eigene Zwecke, wie Werbung nutzen!

Man braucht unbedingt beim Hochladen eines fremden Bildes das Nutzungsrecht, welches man auch kaufen kann.

Prävention: (Vorbeugung)

- ↳ Überlege genau, was du hochlädst (Telefonnummern, Adressen, etc.).
- ↳ Verbreitete die Aufklärung über Datensicherheit.
- ↳ Achtung vor Fake-Identitäten.

Prevence: „Můj profil = Můj obraz!!!!“

- Facebook používá všechny informace Vámi zveřejněné, zadané, uložené....;
- Facebook-Software umí určit identitu člověka prostřednictvím dalších informací: např.: místo, škola, přátelé.....;
- Facebook využívá všechny informace k dalším účelům: k reklamě, k nabízení zboží a služeb (třeba použití telefonních čísel apod.).

Proto je nutné dodržovat přísná bezpečnostní pravidla, při práci na IT sítích:

- Osobní údaje - nikam nedávat údaje (tel. čísla, adresa, č.úctu).
- Žádné nevhodné (intimní) fotky
 - ↳ nikdy nevíte, kdo se dívá na váš profil (pedofil)
 - ↳ přemýšlet nad tím, co na soc. síti udělám.

- **Zabezpečený účet**

- zabezpečit účet, aby mé příspěvky viděli jen přátelé.
- opatrnost
- dávat si pozor s kým si píšu.
často se za PC schovává někdo jiný, např. fakeprofil)
- nezkoušet všechno, co je na internetu.



Příklad: velice nebezpečná - Modrá velryba! Lidé museli plnit nebezpečné úkoly (např. sebepoškozování, budit se v 4:20, jít na střechu, jít na koleje atd. Poslední úkol byla smrt, ovlivnilo to spoustu lidí s depresemi. Kdyby hráči nesplnili úkol, byli by napadáni na Darkwebu.

- **Autorská práva**

- u veškerých informací, co použijeme je potřeba uvést zdroj.
- pokud chci o někom něco zveřejnit, musím mít od toho dotyčného souhlas!!!!
- **Citát-**„Nedělej ostatním, to co nechceš, aby dělali oni tobě!!!“
- dávat si pozor na fotografování lidí, zesměšňovat jej atd.

Když už se to stane

- Svěřit se! – Nečekat až to bude horší!!!
- Je nutné to říci např.: rodičům, kamarádům, učiteli, psychologovi.
- Nenechat se vydírat
- Šikanátoři začnou vydírat, že zveřejní vaše intimní fotky, ublíží příbuzným atd. a toto jim nemůžeme věřit.
- Nepodřizovat se!
- Neplnit žádné požadavky!
- Nikdy nedržet problémy/ bolesti v sobě!
- Když si všimneme podobné situace u kamarádů, máme: upozornit na to rodiče, učitele, pomoci dotyčnému a určitě se nepřipojovat v šikaně pomocí komentářů.

Existuje způsob, jak se bránit proti projevům úmyslné kyberšikany?

Nedopusťte, aby se z vás stala oběť, a držte se určitých zásad!!!!!!!

- ☞ zachovejte chladnou hlavu a nepropadejte panice ani studu, neuzavírejte se do sebe a nebojte se svěřit blízké osobě;
- ☞ na jakkoliv urážlivé projevy nereagujte, ale uložte je v případě potřeby prokázání kyberšikany;
- ☞ v případě pokračujících nebo stupňujících se útoků informujte rodiče, školu, policii;
- ☞ využijte linku bezpečí.

Malware – Schutz vor Viren

7 Tipps um sich vor Malware zu schützen:

1. Virenschutz/Firewall installieren
2. Updates automatisch installieren, um Sicherheitslücken zu schließen
3. Keine unbekannten Links öffnen!
4. (Wenn doch, Link selbst in den Browser eingeben)
5. Keine persönlichen Daten freigeben
6. PC regelmäßig scannen (falls Verdacht auf ein Virus besteht, dann mit einer Live-CD scannen)
7. Nutzungsbedingungen durchlesen
8. Vorher nachdenken bevor man etwas tut!



Apps zum Schutz vor Viren

Android Smartphone:

- CM Security

IOS Smartphone:

- Mobile Security

Computer:

- Bitdefender



Handlungsmöglichkeiten bei Virenbefall

- Nicht allein versuchen zu reparieren!
- Kein Neustart
- **unbedingt einen Experten aufsuchen!!!**

Viry – Prevence

Antivirové programy – počítačové programy ochrany:

- ***Například:***

1. Avast antivirus
2. AVG antivirus
3. Esetsmartsecurity apod.



- Je velmi důležité si takový program od specializovaných počítačových firem nechat nainstalovat. Ochrání nás to od potíží s viry a zároveň to může zabránit ztrátě určitých dat.

1. Měli bychom přemýšlet nad tím, na který odkaz klikáme
2. Musíme si dávat pozor na zavádějící náhodně zobrazující se okna
3. Měli bychom stahovat jen z prověřených zdrojů
4. Neměli bychom otevírat nedůvěryhodné zdroje
5. Měli bychom si přečíst licenční ujednání
6. Měli bychom být ve střehu před zvláštními e-maily (spamy)
7. Neměl by chybět antivirový program

Co dělat v případě, že se objeví vir:

1. Zatelefonovat expertovi z počítačové firmy, nebo bezpodmínečně nějakého odborníka vyhledat!!!
2. Nainstalovat si antivirus
3. V žádném případě se nepokoušet počítač sám opravit (nerestartovat počítač).

Verschlüsselt/ Sicher chatten

Um verschlüsselt bzw. sicher zu chatten, sollte man schauen, dass man sichere Webseiten/Apps von „guten“ Anbietern zum Chatten nutzt. Eine sichere Seite sollte abhörsicher und nicht manipulierbar sein.

Sichere Programme für den **Computer** zum Chatten sind z.B. Jitsi, Cryptocat und TorChat.

Für das **Smartphone** sind Signal, Treema, Telegram und Hoccer empfehlenswert.

Falls Kinder im Internet chatten, sollten Eltern überprüfen können, wo die Kinder chatten. Dies ermöglicht die App „My Mobile Watchdog“. Trotzdem sollte man immer aufpassen, mit wem man chattet. Es ist nicht sehr empfehlenswert, mit fremden Leuten verschlüsselt zu chatten. Es besteht das Risiko, dass sie einem manipulierte Links mit Abhörprogrammen schicken.

Sollte man den Verdacht haben, mit Abhörviren infiziert zu sein, empfiehlt es sich, dies zuerst einer vertrauten Person zu melden. Dazu ist es empfehlenswert, seine Antivirenprogramme regelmäßig zu aktualisieren, damit der Virus eventuell schnell erkannt wird. (Siehe Punkt 3 Malware)



Šifrování – bezpečné chatování:

- Chcete-li šifrovat a / nebo bezpečně chatovat, měli byste se podívat na zabezpečené webové stránky / aplikace od "dobrých" poskytovatelů chatu.
- Bezpečná strana by měla být bezpečná a bez dozoru. Zabezpečené chatovací programy zahrnují Jitsi, Cryptocat a TorChat pro signál, Treema, telegram a Hoccersmartphony.
- Když děti chatují online, rodiče by měli mít možnost zkontrolovat, kde chatují. To umožňuje aplikaci "My MobileWatch Dog".
- Přesto byste měli vždy věnovat pozornost tomu, kdo je na chatu. Nedoporučuje se uchovávat lidi v šifrované podobě.
- Při odesílání odkazu na poslech programů hrozí nebezpečí, že budete chatovat s cizinci. Pokud si myslíte, že jste napadeni, měli byste nejdříve informovat důvěryhodnou osobu.
- Za tímto účelem se doporučuje pravidelně aktualizovat antivirové programy, které rychle detekují virus.



Kde a jak se kyberšikana objevuje:



1. Útočníci jsou anonymní:

Ve virtuálním prostředí většinou útočníci vystupují pod přezdívkou, používají pro oběť neznámou e-mailovou adresu, telefonní číslo atd. Pro agresora navíc není žádný velký problém vytvářet nové identity. Oběť tak má jen malou šanci přijít na to, kdo na ni útočí.

2. Mění se profil útočníků a profil obětí:

Ve virtuálním světě nezáleží na věku, pohlaví, síle, postavení v sociální skupině (partě) ani úspěšnosti útočníka nebo oběti ve společnosti. Původcem kyberšikany může být každý, kdo má potřebné znalosti informačních a komunikačních technologií, tedy i fyzicky slabý jedinec. Výzkumy ukazují, že útočníci tráví více času na internetu, a to bez dohledu rodičů, kteří se příliš nezajímají o to, k čemu internet jejich děti používají. Útočníky bývají častěji chlapci než dívky s dobrým sociálním statutem. Pachatelé kyberšikany jsou také obvykle původci tradičního šikanování.

3. Mění se místo a čas útoku:

Zatímco u tradiční šikany lze předpokládat, kdy a kde k útoku dojde (např. ve škole, na hřišti), s kyberšikanou se můžeme setkat kdykoliv a kdekoliv. Obětí útoku se můžeme stát vždy, když budeme připojeni k internetu nebo když budeme mít u sebe svůj mobilní telefon. V takovém případě se před kyberútokem nemáme kam schovat. Útočník si nás může najít i v „bezpečí domova“ a klidně to může být i o půlnoci.

4. In einer virtuellen Umgebung verhalten sich

Menschen anders als in der realen Welt:

Täter können mit einem unterschiedlichen Alter, verschiedenem Geschlecht, verschiedenen Berufen bewusst die manipulieren, mit denen Sie kommunizieren. In der virtuellen Welt verhalten sich einige Menschen weniger sorgfältig als in der realen Welt (Sie sind mutiger in der Kommunikation, der Diskussion sensibler Themen, kommunizieren oft ohne Skrupel etc.). Manchmal versuchen sie Dinge, vor denen sie in der realen Welt Angst hätten (z.B. den Angriff auf die andere Person, sie zu bedrohen oder zu erpressen), weil es weniger Risiko ihrer Entdeckung gibt. Sie sehen nicht, was die Auswirkungen ihres Verhaltens auf die Opfer sind, vor allem, wenn wir erkennen, dass die Opfer nach dem Zufallsprinzip ausgewählt werden, somit sie sich nicht unbedingt persönlich kennen.

5. Wenn die Zielgruppe hilft, Cyber-Mobbing zu verbreiten:

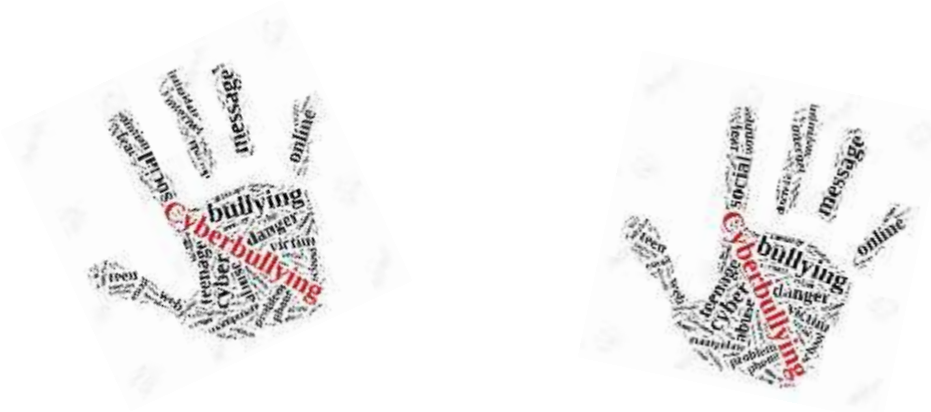
Cybermedien (Bericht und Aufzeichnungen) können sehr einfach verbreitet werden. Cybermobbing kann daher ein sehr großes Publikum haben. Der Angreifer braucht sein Opfer nicht wiederholt zu attackieren. Es werden einfach sensible Nachrichten oder Aufnahmen im Internet veröffentlicht und um ihre Verbreitung kümmern sich andere. Dieses "Publikum" ermöglicht es ihm dann, die Intensität des Angriffs zu erhöhen und die Auswirkungen auf das Opfer zu verstärken.

6. Die Auswirkungen von Cyberbullying auf das Opfer sind nicht leicht zu erkennen:

Cybermobbing ist meist verbunden mit psychologischer Misshandlung der Opfer. Diese ist nicht leicht zu erkennen (anders als blaue Flecken, die körperliches Mobbing begleiten). Opfer von Cybermobbing ziehen sich oft zurück und kommunizieren ihre Probleme nicht mit anderen. Die Gründe für ein solches Verhalten können tiefer liegen: Angst,

IT slabikář vychází za podpory Česko-německého fondu budoucnosti.
Herausgegeben mit freundlicher Unterstützung des Deutsch-Tschechischen Zukunftsfonds.

Scham, die Eltern verstehen die Computertechnik nicht, ein Kind erkennt nicht, dass es an einer Manifestation von psychischem Mobbing leidet etc.). Für die Lösung ihrer Probleme bleiben die Opfer meist auf sich gestellt, das kann dazu führen, dass sie scheitern und die Situation nicht verarbeiten.



Dobré rady, co udělat, pokud na nás někdo útočí přes sociální síť:

1. Pokud se stanete obětí kyberšikany, schovejte kopie všech útočnickových e-mailů, textových zpráv a internetových aktivit. Mohou pomoci při hledání agresora
2. Máte-li mezi spolužáky nebo kamarády nějaké problémy, řešte je osobně, ne elektronicky!
3. Pokud na vás někdo prostřednictvím určité služby útočí, použijte nástroje, které poskytovatel pro takový případ vytvořil. Například na Facebooku můžete nastavit kdo a co z vašeho profilu může sledovat. Případně můžete provozovatelům služby nahlásit nevhodný obsah (ať už hanlivý, rasistický nebo pornografický).

Gute Ratschläge, was zu tun ist bei einem Angriff über soziale Netzwerke:

1. Wenn Sie ein Opfer von Cyber-Mobbing sind, speichern Sie Kopien aller attackierenden Emails, SMS-Nachrichten und Internetaktivitäten. Sie können bei der Suche nach dem Angreifer helfen.
2. Wenn Sie mit Mitschülern oder Freunden irgendwelche Probleme haben, wenden Sie sich bitte persönlich und nicht elektronisch an diese!
3. Wenn Sie jemand durch einen bestimmten Dienst angreift, verwenden Sie die Tools, die der Anbieter für einen solchen Fall bereitstellt. Zum Beispiel können Sie auf Facebook festlegen, wer was von Ihrem Profil sehen kann. Alternativ können Sie dem Betreiber unangemessene Inhalte melden (ob diffamierend, rassistisch oder sexuell).



KDE HLEDAT POMOC nebo KAM SE OBRÁTIT?

- **INTERNETOVÁ PORADNA** "Projektu E-Bezpečí" nebo **MÁŠ PROBLÉM?**
Web: www.e-bezpeci.cz
- **Linka BEZPEČÍ ONLINE (Internet Helpline)**

Tato asistenční linka je zaměřena na oběti internetové kriminality. Na Internet Helpline mohou děti či dospělí ohlásit zneužívání dětí při komunikaci na internetu (např. v rámci kyberšikany, kybergroomingu, kyberstalkingu apod.). Odborní konzultanti obětem poskytnou nezbytnou psychosociální pomoc a také jim poradí, jak bezpečněji internet používat.

Telefonní číslo: 116 111

Web: www.internethelpline.cz

- **KRIZOVÁ TELEFONNÍ linka IPPP ČR**
- Krizová linka Institutu pedagogicko-psychologického poradenství ČR poskytuje pomoc při řešení případů šikany/kyberšikany, ale i v dalších krizových situacích. Na linku se mohou obracet učitelé, žáci i rodiče. Pracovníci linky pomoc poskytnou nebo zprostředkují.
Telefonní číslo: 286 881 059 nebo +420 774 089 181
- **NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU**
Web: www.saferinternet.cz



Mobbing – Was tun?

Prävention

1. Persönliche Vorsorge



Man sollte nicht unüberlegt persönliche Daten und Darstellungen von sich preisgeben. Leute die schon einmal selbst andere gemobbt haben oder in Chaträumen aktiv sind werden schneller zu Mobbingopfern.

2. Durch Aufsichtspersonen

Indem Erwachsene das Selbstbewusstsein der Kinder/Jugendlichen stärken, können sie Mobbing vorbeugen. Auch durch das Aufklären über Gefahren.

3. Firmen und Institutionen

Auch soziale Netzwerke starten ab und zu Aufklärungsaktionen. Außerdem werden „Notfallbuttons“ installiert, mit denen Gefahren direkt gemeldet werden können.

Gegenmaßnahmen

1. Zivilcourage

Damit das Internet zu einem sicheren Ort wird, sollte man nicht wegschauen und helfen. Man sollte immer daran denken, dass man auch selbst zum Mobbingopfer werden könnte und dann dankbar für Hilfe wäre.

2. Abwehr

Man sollte die Kommentare, Seiten und Profile melden und möglichst schnell die Eltern bzw. die Polizei informieren. Umso länger man wartet, desto schlimmer und stärker wird das Mobbing.

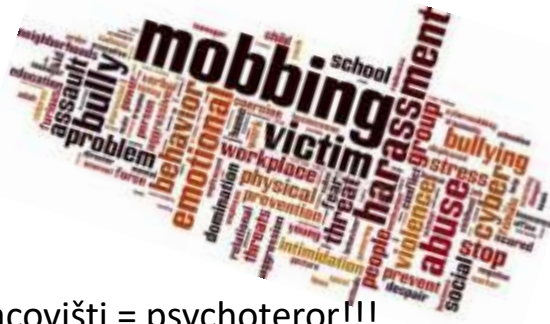
3. Erste Hilfe, Selbsthilfe

Es gibt Selbsthilfeplattformen, wie z.B. juuport.de auf denen 14-18 jährige mit psychologischer Ausbildung Tipps geben. Einigen fällt es leichter mit Gleichaltrigen zu reden, als mit Eltern.



Kyberšikana

Mobbing:



Definice - Je druh šikany na pracovišti = psychoteror!!!

- Mobbing = hromadně napadnout
- mobbing označuje různé formy znepríjemňování života na pracovišti
- typická je skrytost této šikany
- někdy se objevuje mobbing jako sexuální obtěžování na pracovišti
- variantou šikany může být také bossing- je specifický tím, že se šikany, dopouští nadřízený, tento typ šikany zhoršuje vztahy na pracovišti
- za šikanu může být považováno:
 - a) přehnané kontrolování ze strany nadřízeného
 - b) neschválení dovolené a přestávek
 - c) arogantní chování
 - d) kritika

Prevence - Mobbing = **Co dělat?**

1. Osobní opatrnost dospělého – jsem sám za sebe zodpovědný, musím být opatrný a přemýšlet o své činnosti
2. Dohlížející osoby – rodiče, učitelé... měli by vždy vědět a být mladistvým nápomocni s tím, co oni na sítích dělají, s kým chatují.... Měli by s dětmi o problému hovořit a vysvětlovat tuto problematiku.
3. Firmy a instituce- na sociálních sítích startují občas vysvětlující kurzy. Také instalace kvalitních, antivirových programů je velmi dobré a účinné.

Co bychom si měli uvědomit a co je důležité:

Osobní odvaha = vyhledat pomoc, překonat strach!!!

Obrana:

- informovat rodiče
- informovat policii, učitele
- komentáře, profil, zpráva atd...
- opatrnost při práci!!!

Reakce:

- rychlé působení, rychlá obrana
- nejdřív pomáhej sobě!
- jak si mohu pomoci sám?

Opatrnost:

- osobní
- žádná osobní prezentace
- opatrnost na ostatní útočníky na chatovacích programech.
- podle dozoru:(učitel, rodič)
- posílení sebevědomí mladistvých
- je nutné dětem od malička vysvětlovat nebezpečí, které hrozí na internetu
- firmy a instituce ve svých programech vysvětlují dětem, že nemají klikat na vše, co vidí = nebezpečí může přijít i přes ikony (viry).



Gefährliche Internettrends

Die Blue Whale Challenge

Der Name ist abgeleitet von dem Freitod welchen auch Wale betreiben, indem sie auf den Strand zuschwimmen und dort verenden.

Teilnehmer ritzen sich einen Wal in die Handfläche als Erkennungszeichen.

Freitod ist ebenfalls Ziel der Teilnehmer.

Jeden Tag eine der 50 außergewöhnlichen Aufgaben erfüllen.

Zum Beispiel

- ↳ mitten in der Nacht auf ein Dach klettern
- ↳ bestimmte Filme anschauen
- ↳ sich selbst verletzen
- ↳ Die letzte Aufgabe ist der Tod

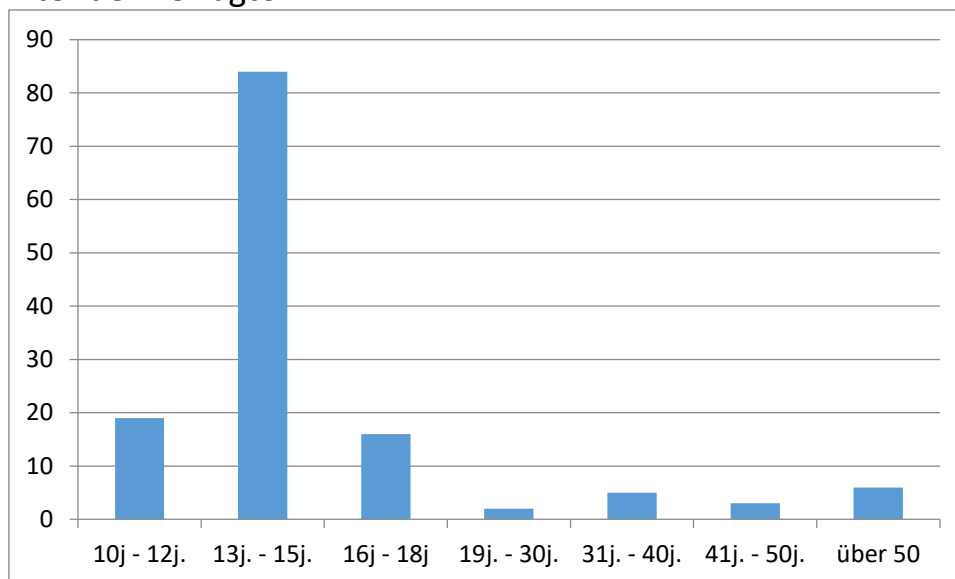
Anfangs auf „Vkontakte“ russisches Pendant zu Facebook .

90-130 Jugendliche starben dadurch.

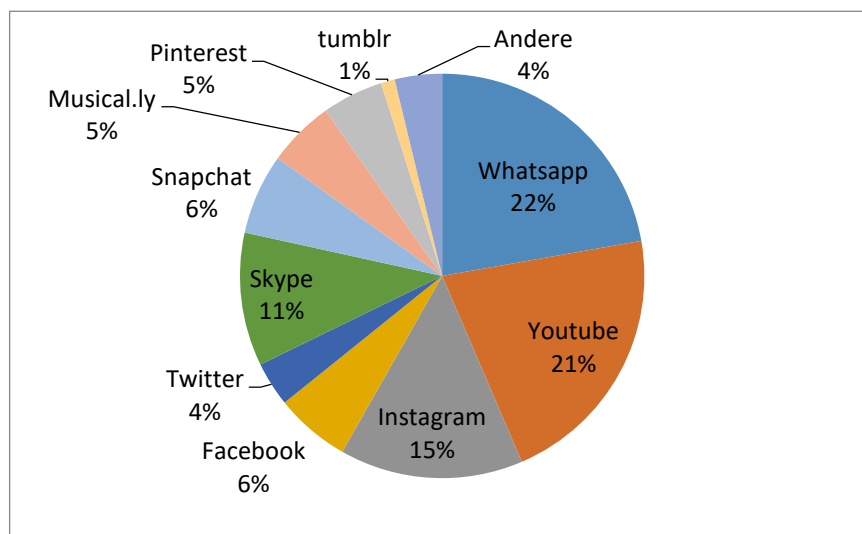
Es ist ungeklärt ob, das Internet-Phänomen zum Selbstmord geführt hat oder ob es von vornherein labile Jugendliche waren, die eine Suizidoption gesucht haben.

Auswertung Umfrage Augustusburg

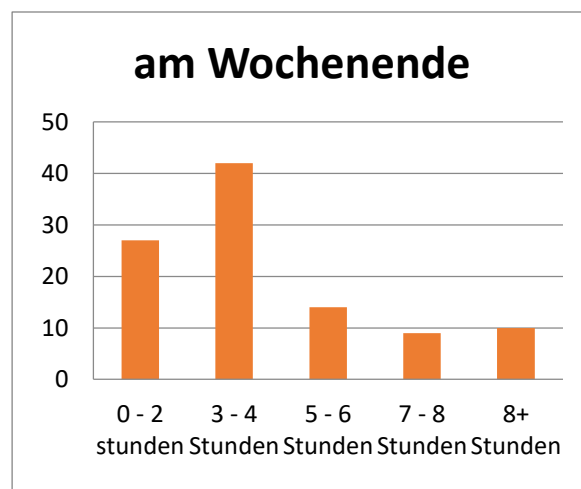
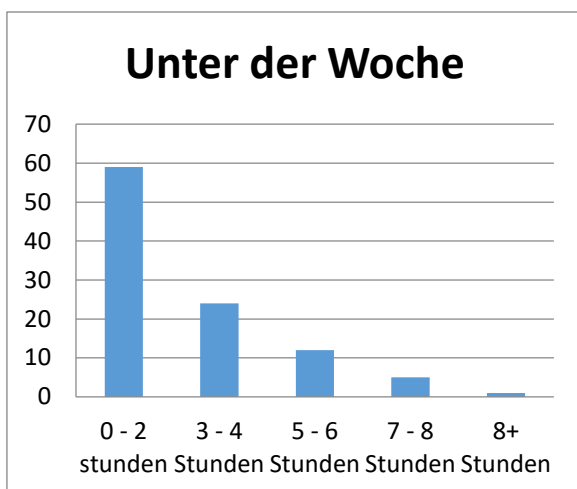
0. Alter der Befragten



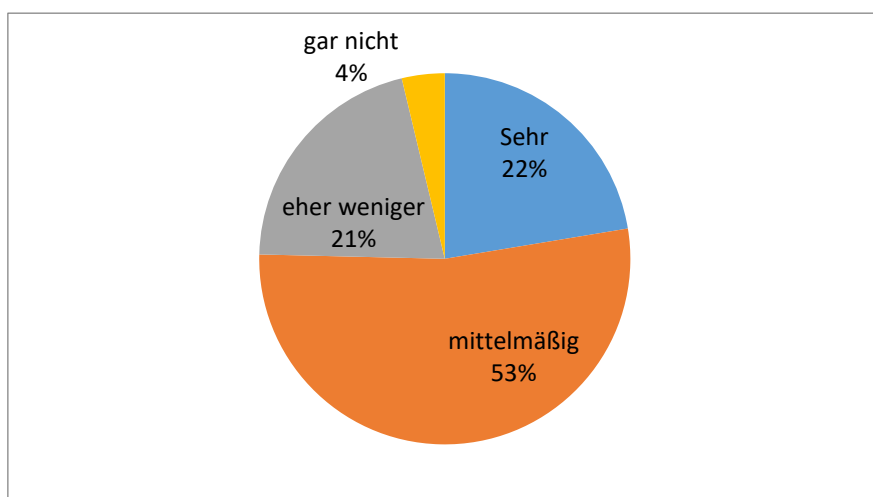
1. Welche Social Media Netzwerke werden benutzt?



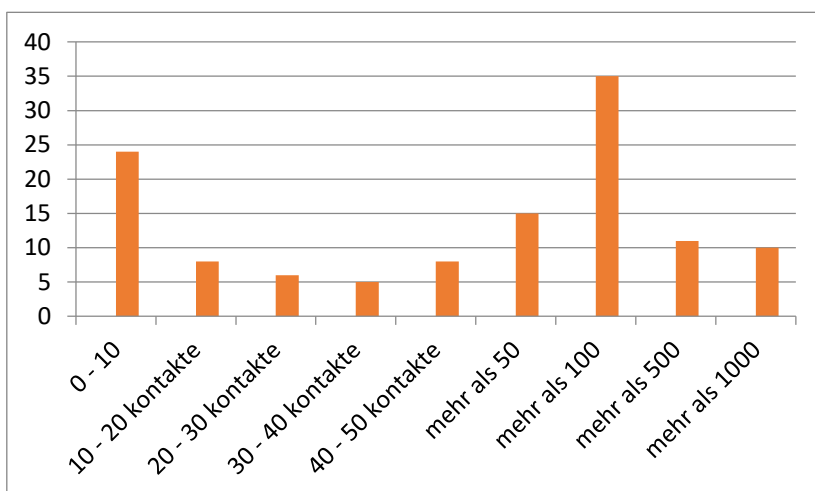
2. Wie oft werden sie unter der Woche und am Wochenende benutzt?



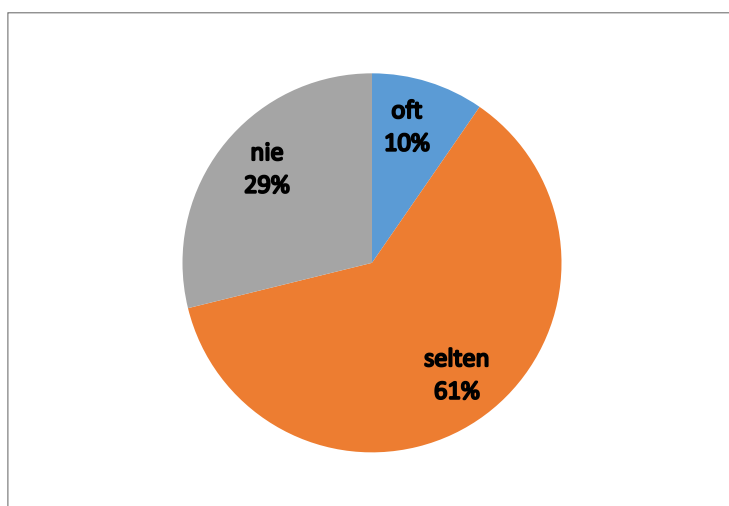
3. Wie wichtig sind die Social Media Netzwerke?



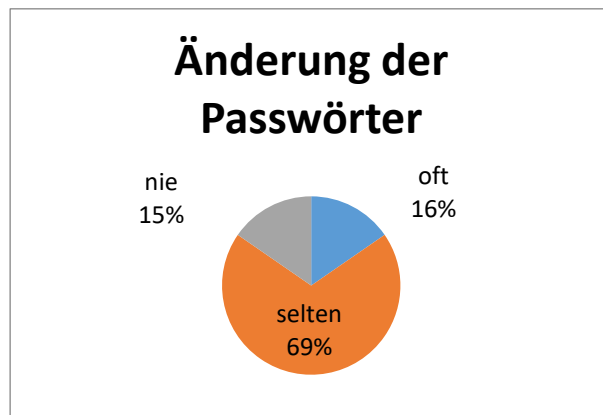
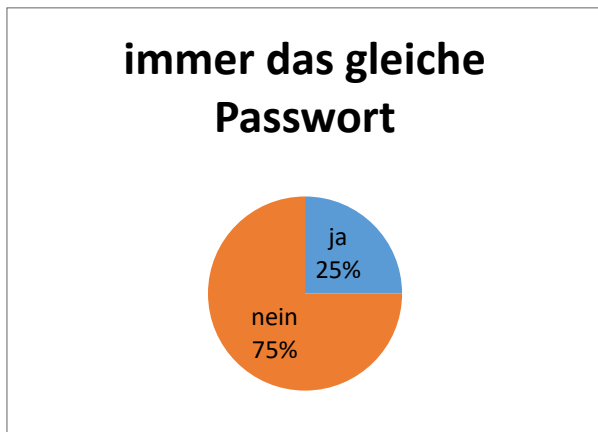
4. Wie viele Follower haben die Befragten



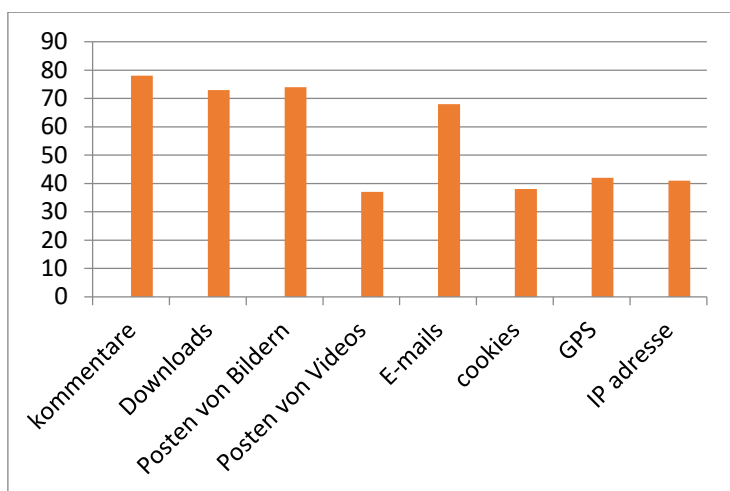
5. Wird sich oft mit öffentlichen Hot-Spots verbunden?



6. Werden die Passwörter oft geändert, bzw. werden immer die gleichen Passwörter benutzt?



7. Welche Spuren, glauben die Befragten, werden im Internet hinterlassen?

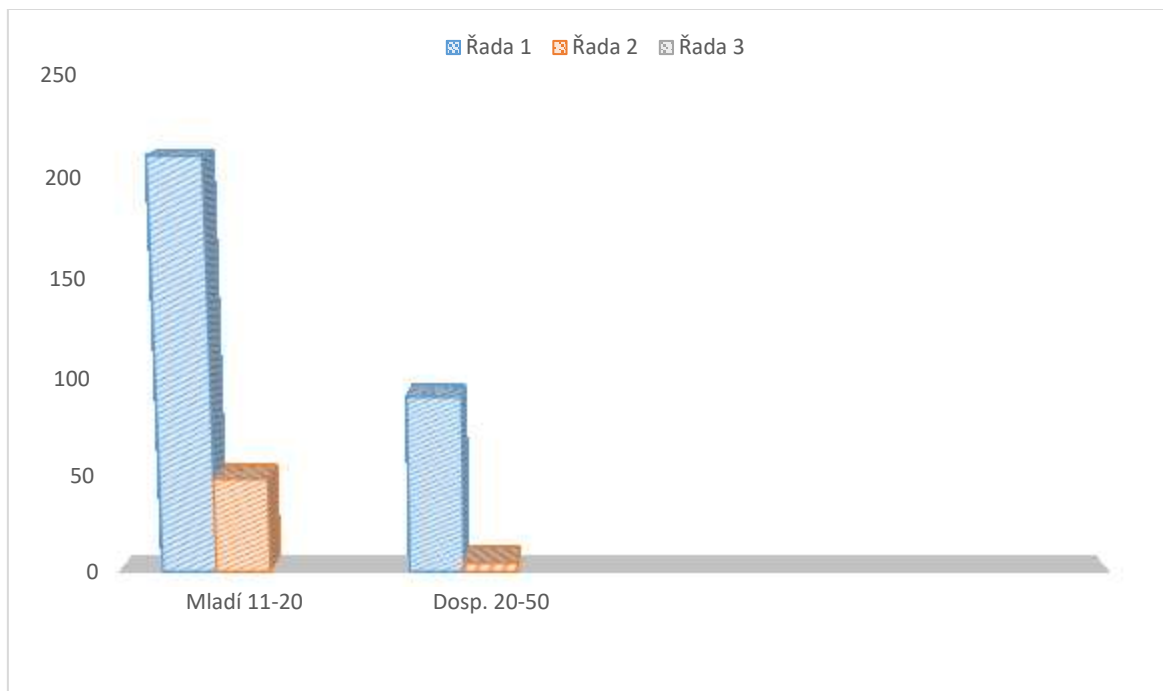


Graf kyberšikana:

Celkově se ankety zúčastnilo 346 lidí.

1. mladí lidé ve věku 11 - 20 let: celkem **210**.
 - z toho **48** se setkala s kyberšikanou
2. dospělí lidé ve věku 20 - 50 let: celkem **90**.
 - z toho **8** se setkala s kyberšikanou

Graf č. 1 Kolik lidí různého věku se setkala s kyberšikanou:



- ve skupině č.1 - tedy - u mladých lidí je to **23%**
- ve skupině č.2 - tedy – dospělých je to **9,8%**

Z našeho grafu vyplývá, že mladí lidé se stávají obětí kyberšikanou podstatně více, než lidé starší.

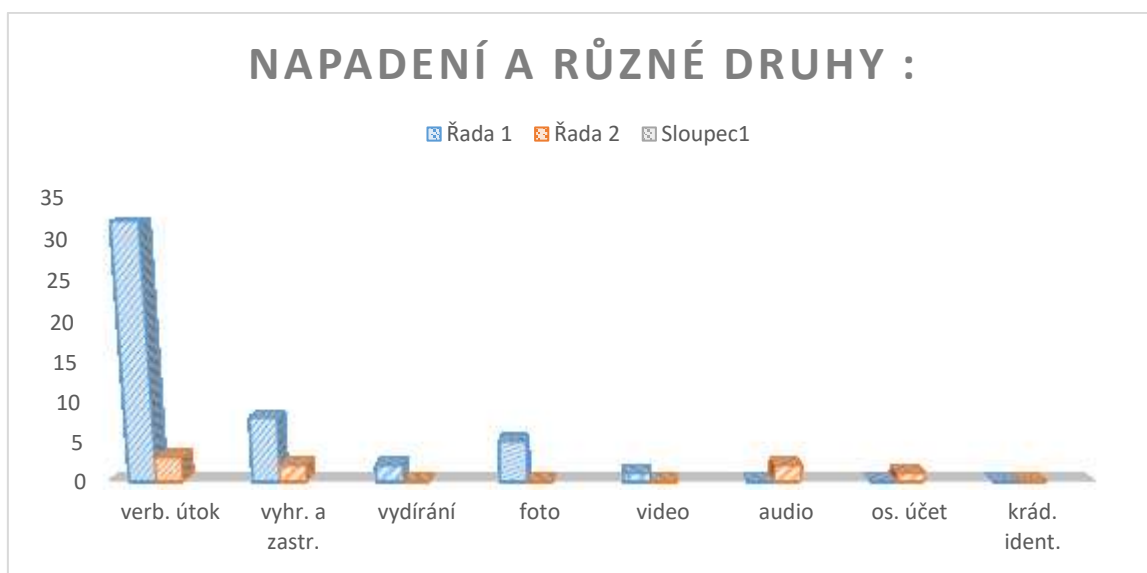
Je to tím, že jsou častěji a déle na sociálních sítích. Proto je důležitá prevence a osvěta.

Také je důležité zabývat se tím, jakým způsobem se dotyční s kyberšikanou setkali.

A tímto se zabýváme v našem druhém grafu, kde jsme se snažili zjistit s jakým druhem kyberšikanou a jakém věku se s ní lidé z ankety setkali.

Druhy napadení:

1. Verbální útok
2. Vyhrožování a zastrašování
3. Vydírání
4. Ponižování a ztrapňování šířením fotografie
5. Ponižování a ztrapňování šířením videa
6. Ponižování a ztrapňování šířením audia
7. Napadení osobního účtu
8. Krádež identity



Arten von Angriffen:

1. Verbaler Angriff
2. Drohungen und Einschüchterung
3. Erpressung
4. Demütigung und Peinlichkeit durch die Verbreitung der Fotografie
5. Demütigung und Peinlichkeit durch die Verbreitung des Videos
6. Demütigung und Peinlichkeit durch die Verbreitung des Audios
7. Persönlicher Kontoangriff
8. Identitätsdiebstahl

Teilnehmer

Bronold	Luise	11.09.2002
Burkhardt	Maja	15.08.2002
Heinrich	Leoni-Shirin	20.12.2002
Hentschel	Hannah Sophie	04.04.2003
Stoll	Mathilde	28.05.2003

Hendel	Friederike	18.07.2002
Henzschel	Zoe Michelle	24.08.2002
Juds	Anna Kiera	19.08.2002
Kunert	Selina	28.10.2002
Steuer	Michelle	10.12.2002
Zinner	Niclas	05.02.2003

Eliška	Herzigová	10.05.2001
Karolína	Kinštová	06.02.2001
Tereza	Kolkopová	04.05.2000
Kevin	Rauschnik	19.07.2001
Jakub	Suk	21.08.2001
Kristina	Volfová	21.02.2001
Kateřina	Rakašová	14.04.2001
Karolína	Koreňová	25.01.2000
Lenka	Moučková	11.04.2001
Ivana	Hořejší	04.09.2000

Použité stránky:

<https://www.e-bezpeci.cz/index.php/temata/kyberikana/17-cojekyllersikana>

IT slabikář vychází za podpory Česko-německého fondu budoucnosti.
Herausgegeben mit freundlicher Unterstützung des Deutsch-Tschechischen Zukunftsfonds.

