Інфармацыю пра асоб знайдзіце самастойна, выкарыстоўваючы пошук у Інтэрнэце (пры неабходнасці перавядзіце тэкст на беларускую мову). Для ўстаўкі відарысаў выберыце кнопку  Найти в Интернете.

7* З дапамогай сэрвісу Google **Формы** стварыце анкету на адну з пералічаных тэм (групавая работа).

1. Здаровы спосаб жыцця.
2. Захапленні і спорт.
3. Мая будучая прафесія.
4. Край, у якім я жыву.

Разашліце анкету (кнопка ОТПРАВИТЬ) аднакласнікам на электронную пошту.

Заўвага. Прадугледжваецца работа ў групах.

§ 5. Сеткавы этыкет і меры бяспекі ў сетцы Інтэрнэт

У Інтэрнэце часта выкарыстоўваюць спецыяльныя словы (слэнг).

1. Для абазначэння парушэнняў правіл сеткавага этыкету:

Флэйм (англ. *flame* — полымя) — нечакана ўзнікшае актыўнае абмеркаванне, пры развіцці якога ўдзельнікі звычайна забываюць пра першапачатковую тэму, пераходзяць на асобы і не могуць спыніцца.

Флуд (англ. *flood* — паводка) — паведамленні, якія не нясуць ніякай карыснай інфармацыі. Флуд можа распаўсюджвацца з мэтай тролінгу, г. зн. з прычыны жадання каму-небудзь дапячы. Тэхнічны флуд уяўляе сабой хакерскую атаку з вялікай колькасцю запытаў, якая прыводзіць да адмовы работы сэрвісу (DDoS-атака).

Спам (англ. *spam*) — паведамленні, якія прыходзяць ад невядомых людзей або арганізацый без дазволу. Часта тэрмін *спам* ужываецца ў значэнні *паштовы спам* — рассылка электронных лістоў, якія змяшчаюць рэкламу.

Афтоп (англ. *off topic* — па-за тэмай) — сеткавае паведамленне, якое не мае адносін да загадзя вызначанай тэмы зносін. Формай афтопа, якая найменш ухваляецца, з'яўляюцца рэкламныя паведамленні.

Інтэрнэт — свет цікавых і карысных магчымасцей, але ў той жа час гэта крыніца пагроз, асабліва для дзяцей і моладзі. Агрэсія, махлярства, псіхалагічны ціск — небяспекі, якія могуць чакаць у глабальнай сетцы кожны дзень.

У 6-м класе вы пазнаёміліся з сеткавым этыкетам пры рабоце з электроннай поштай, даведаліся, якія меры бяспекі неабходна выконваць, карыстаючыся электроннай паштовай скрынкай. Працуючы з рознымі воблачнымі сэрвісамі ці маючы зносіны па сетцы, трэба выконваць такія ж правілы, як і пры рабоце з электроннай поштай.

Абязлічанасць пры зносінах у Інтэрнэце прымушае карыстальнікаў забываць, што яны маюць справу не з машынай, а з рэальнымі людзьмі. Правілы сеткавага этыкету дапамагаюць дасягнуць узаемаразумення і забяспечваюць бяспеку зносін. Асноўныя з іх:

1. Будзьце ветлівыя і не забывайце пра абавязковыя формулы прывітання, звароту, падзякі.

2. Пазбягайце беззмястоўных гутарак, каб не марнаваць свой час і час суразмоўцы.

3. Пішыце пісьменна. Выкарыстоўвайце праверку арфаграфіі. Перад адпраўкай паведамлення перачытайце тэкст.

4. Без неабходнасці не пішыце на трансліце (г. зн. не злоўжывайце выкарыстаннем літар алфавіта іншай мовы). Не набірайце тэкст вялікімі літарамі. Не перагружайце паведамленне смайлікамі.

5. Захоўвайце ананімнасць пры зносінах з незнаёмцамі.

Неабачлівасць і нядбайны падыход да забеспячэння бяспекі ў Інтэрнэце можа даць магчымасць злачынцам здзейсніць супрацьпраўныя дзеянні. Спачатку злачынец атрымлівае несанкцыянаваны доступ да ўліковых запісаў у сацыяльных сетках, да электроннай паштовай скрынкі, да акаўнтаў і інш. Атрымаўшы рэквізіты, зламыснік заходзіць ва ўліковы запіс і ажыццяўляе рассылку кантактам уладальніка ўзламанага ўліковага запісу паведамленні ашуканскага характару.

Рэкамендацыі, якія дапамогуць знізіць верагоднасць здзяйснення супрацьпраўных дзеянняў у Інтэрнэце:

1. Для выхаду ў сетку Інтэрнэт выкарыстоўвайце ўстройствы, на якіх установлены і ўвесь час абнаўляюцца антывірусныя праграмы.

2. Пры наведванні вядомых сайтаў звяртайце ўвагу на іх знешні выгляд: магчыма, гэта падробленая копія.

3. Уводзьце асабістую інфармацыю толькі на вэб-сайтах, якія працуюць з выкарыстаннем ахаваных пратаколаў

Хотлінк (англ. *hotlink*) — уключэнне ў вэб-старонку файлаў-відарысаў або іншых рэсурсаў з чужога сервера. Гэты прыём выкарыстоўваецца нядобрасумленнымі вэб-майстрамі. Пры гэтым трацяцца чужыя рэсурсы і трафік.

Аверквотынг (англ. *overquoting*) — залішняе цытаванне.

2. Для абазначэння супрацьпраўных дзеянняў у Інтэрнэце:

Фішынг (англ. *phishing* — *password* + + *fishing* — вывуджванне пароляў) — від махлярства з мэтай атрымання доступу да лагінаў і пароляў карыстальнікаў.

Кіберсквотынг (англ. *cybersquatting*) — рэгістрацыя даменных імёнаў, якія змяшчаюць гандлёвую марку, што належыць іншай асобе, з мэтай іх далейшага перапродажу ці нядобрасумленнага выкарыстання.

Брутфорс (ад англ. *brute force* — поўны перабор) — метад атакі або ўзлому шляхам перабору ўсіх магчымых варыянтаў пароля.

Кардынг (ад англ. *carding*) — від махлярства з выкарыстаннем чужой плацежнай карты ці яе рэквізітаў.

Клікджэкінг (англ. *clickjacking*) — механізм падману карыстальнікаў Інтэрнэту, які дазваляе даведацца кантакты наведвальнікаў сайта яшчэ да таго, як яны самі змясцілі іх на сайце.

Руткіт (англ. *rootkit*) — праграма ці набор праграм для ўтойвання слядоў прысутнасці зламысніка ці шкоднай праграмы ў сістэме.

Фармінг (англ. *pharming*) — схаванае перанакіраванне на няправільны IP-адрас.

Прыклады махлярства ў Інтэрнэце:

1. Ажыццяўляецца вірусная атака на камп'ютарныя ўстройствы, блакіруецца браўзер ці аперацыйная сістэма, а на экране манітора з'яўляецца патрабаванне аплаціць буйны штраф.

2. На электронную паштовую скрынку прыходзіць ліст, які абяцае: пасля куплі вучэбнага курса можна ўжо заўтра пачынаць зарабляць вялізныя грошы. Памятайце, што ніхто не будзе расказваць зусім незнаёмым людзям, як зарабіць вялізныя грошы, махляры проста зарабляюць грошы на продажы гэтых вучэбных курсаў.

Прыклад 5.1. Артыкулы Крымінальнага кодэкса Рэспублікі Беларусь, якія вызначаюць адказнасць за злачынствы ў сетцы Інтэрнэт (http://kodeksy.by).

Артыкул 212. Крадзеж шляхам выкарыстання камп'ютарнай тэхнікі.

Артыкул 349. Несанкцыянаваны доступ да камп'ютарнай інфармацыі.

Артыкул 350. Мадыфікацыя камп'ютарнай інфармацыі.

Артыкул 351. Камп'ютарны сабатаж.

Артыкул 352. Неправамернае завалоданне камп'ютарнай інфармацыяй.

Артыкул 353. Выраб або збыт спецыяльных сродкаў для атрымання неправамернага доступу да камп'ютарнай сістэмы ці сеткі.

Артыкул 354. Распрацоўка, выкарыстанне або распаўсюджванне шкодных праграм.

Артыкул 355. Парушэнне правіл эксплуатацыі камп'ютарнай сістэмы ці сеткі.

Аналіз 3 млн створаных людзьмі васьмізначных пароляў паказаў, што літара «e» была выкарыстана ў паролях 1,5 млн разоў, у той час як літара «f» — толькі 250 000 разоў.

Рэсурс для праверкі ўнікальнасці пароля: https://exploit.in/passcheck

(у браўзеры побач з адрасам такога сайта адлюстроўваецца значок замка).

4. Не выкарыстоўвайце аднолькавыя лагіны і паролі на розных сайтах.

5. Не выкарыстоўвайце лёгкія паролі (даты нараджэння, нумары тэлефонаў і г. д.).

6. Сцеражыцеся нечаканых ці незвычайных электронных паведамленняў, нават калі вам вядомы адпраўшчык; не адкрывайце ўлажэнні і не пераходзьце па спасылках у такіх паведамленнях.

7. Пры паступленні паведамленняў ад знаёмых, якія змяшчаюць просьбы пра фінансавыя аперацыі ці пра перадачу фінансавых рэквізітаў, абавязкова правярайце дадзеную інфармацыю па іншых каналах сувязі (асабістая сустрэча, тэлефонны званок, галасавая сувязь). Паспрабуйце вызначыць асобу суразмоўніка з дапамогай кантрольных пытанняў, адказы на якія могуць быць вядомыя толькі вам дваім.

Заканадаўствам Рэспублікі Беларусь вызначана мера адказнасці за наступныя злачынствы ў сетцы Інтэрнэт:

1. Несанкцыянаваны доступ да даных.

2. Мадыфікацыя (змяненне) даных без дазволу ўладальніка.

3. Наўмыснае знішчэнне даных, прывядзенне іх у непрыдатны стан.

4. Распрацоўка, выкарыстанне і распаўсюджванне шкодных праграм.

5. Парушэнне аўтарскага права.

(Разгледзьце прыклад 5.1.)

1. Чаму трэба выконваць правілы этыкету пры зносінах у сетцы Інтэрнэт?
2. Якія правілы сеткавага этыкету не выконваюцца ў прыведзеных ніжэй паведамленнях?

Сёння чацвер. Гэта горш, чым субота, але значна лепш, чым панядзелак... Але крыху горш, чым пятніца. Затое чацвер лепш, чым серада. Чацвер нават лепш, чым нядзеля, таму што ў нядзелю заўтра панядзелак, а ў чацвер заўтра пятніца...

Смайлы 😀😀😀 — гэта вельмі зручна 👍👍. Але ў той жа час у іх ёсць адваротны бок 😟. Яны захоўваюць гэтую тайну 🤐🤐. І ніхто не павінен ведаць пра яе 🤐🤐. НІХТО! 🤐🤐🤐

нАмаЛюй Мне:
1) пАвАжАеШ — рУжоВы фОн;
2) ПаКрыЎдзіЎся — КарычНевЫ фОн;
3) сябрУеш — бЕлЫ фОн.
рАзашлІ гЭта Ўсім СвАім СяБРаМ, І тВая СцЯнА бУдзЕ СупеРПрыГоЖая.

3. Якія меры неабходна прыняць, каб засцерагчы свае ўліковыя запісы ад дзеянняў махляроў?
4. Якім павінен быць бяспечны пароль?
5. Якія дзеянні ў сетцы Інтэрнэт вызначаны заканадаўствам Рэспублікі Беларусь як супрацьпраўныя?

Практыкаванні

1 Прывядзіце прыклады, калі выконваюцца і не выконваюцца правілы сеткавага этыкету. Зрабіце вывад.

2 Выберыце з табліцы небяспечныя паролі.

sdfghjkl	password	qS8+njiPh	12345678	Yn2004

Стварыце тэкставы дакумент, які змяшчае тлумачэнне вашага выбару для кожнага пароля.

3 Падрыхтуйце прэзентацыю на тэму «Сеткавы этыкет».

4 З дапамогай сэрвісу Google **Формы** стварыце анкету на тэму «Бяспека ў сетцы Інтэрнэт».