**ІНТЕРНЕТ - ЗАГРОЗИ ТА БЕЗПЕЧНЕ ПОВОДЖЕННЯ В МЕРЕЖІ**

 Під час дистанційного навчання найбільш зручним способом одержання й передачі різноманітної інформації є використання всесвітньої комп'ютерної мережі Інтернет. Поряд із своїми позитивними сторонами, він являється одним із джерел особистої і комп’ютерної небезпеки. На жаль, багато користувачів не знають про ймовірні загрози та правила безпеки у інтернеті. Розглянемо їх.

**Загрози мережі Інтернет**

***1. Фішинг***

 Фішинг — це схема, за якої шахраї змушують користувачів передавати персональні дані. Найулюбленіший спосіб шахраїв - отримати доступ до вашої банківської картки. На ваш мобільний телефон надходить дзвінок, людина представляються працівником банку і починає з вами бесіду в ході якої розвідує вашу конфіденційну інформацію, щоб згодом використати її для доступу до ваших заощаджень. Запам’ятайте назавжди, жоден банк ніколи не дозволить своїм працівникам шляхом використання телефонії спілкуватися на тему ваших конфіденційних даних. Дзвінок може носити лише інформативний характер, вимагати від вас можуть лише кодове слово, яке ви повідомляли у фінустанові в якості паролю, щоб підтвердити певні дії з вашими картками. Тому, якщо вам телефонують з банку, у жодному разі не повідомляйте ніяких даних про себе і свої карти – вся потрібна інформація у них присутня. І ні в якому разі ніде і ніколи не повідомляйте нікому три цифри (CVC-код), що на звороті вашої карти і строк її дії.

 ***2. Кібербулінг***

 Це розповсюдження принизливої, часто неправдивої інформації через текстові повідомлення, фото, відео з використанням засобів електронного

зв’язку, знімання на відео реальних нападів з метою їх поширення в інтернет мережі, надсилання повідомлень, які ображають когось або погроз. Кібербулінг - неодноразова поведінка, спрямована на залякування, провокування гніву чи приниження тих, проти кого він спрямований.

 ***3. «Допомога рідним»***

Багатьом відома історія, про те, коли людині надходить дзвінок і особа нерозбірливим, але збентеженим голосом повідомляє вам, що це ваш родич, він потрапив у халепу і йому потрібна поміч грошима. Шахраї, зазвичай, б'ють на емоції та переконують: діяти потрібно терміново, і кожна секунда затримки - може вартувати життя. Завдання афериста - викликати стрес і змусити людину, вимкнувши розум, керуватися емоціями. Перед тим, як почати панікувати, поставте якомога більше запитань людині, що вам телефонує. Аналізуйте усе почуте. Іноді досить лише одного запитання - «У яке місто Ви телефонуєте?», аби співрозмовник по той бік слухавки завершив діалог. Не поспішайте перераховувати гроші на вказаний номер або віддавати їх особі, обов`язково передзвоніть "постраждалому".

*** 4. «Виграш»***
Ще один різновид фішингу. Вам надходить дзвінок в процесі якого повідомляють, що ви стали учасником акції чи переможцем. В ході спілкування виявляється, що для того, щоб забрати приз, треба або десь зареєструватися, або внести страховий платіж тощо. Для реєстрації сервіс вимагатиме від вас персональні дані та картковий рахунок, начебто для видачі призу у грошовій формі на вашу банківську картку Ви маєте вказати: номер картки, код CVC, термін дії картки і номер телефону. Також зловмисники можуть розповідати, що для того щоб отримати подарунок – потрібно протягом певного строку сплатити страховий платіж у невеликому розмірі. Якщо внесете дані або перерахуєте гроші, ви станете жертвою шахраїв.

**Основні правила безпечної поведінки в Інтернеті**

 1. Не розголошуйте свої персональні дані та дані інших людей (прізвище, ім’я, по-батькові, дату народження, дані документів, номери телефонів, домашню адресу та ін.) – усе це можуть використати зловмисники.

 2. Будуй власну онлайн-репутацію, не провокуйся ілюзією анонімності. Інтернет – це особливе середовище із своїми правилами поведінки - «нетикетом». Хоча кіберпростір і надає додаткові можливості відчути свободу і розкутість завдяки анонімності, існують способи довідатись, хто саме відправив повідомлення, хто стоїть за певним ніком. І якщо некоректні дії у віртуальному просторі призводять до реальної шкоди – від анонімності залишається лише ілюзія: все тайне стає явним. У віртуальному просторі, як і в реальному, діє золоте правило: стався і дій стосовно інших так, як хотів би, щоб ставились до тебе. Крім того, Інтернет фіксує історію, яка складається із публічних дій учасників і визначає його онлайн-репутацію – накопичений образ особистості в очах інших учасників: заплямувати її легко, виправити – важко.

 3. Якщо ви зіткнулися з кібербулінгом, зберіжить підтвердження факту нападів та обов`язково повідомте про це батьків, соціально - психологічну службу центру, майстра в/н або класного керівника. Часто можна почути думки накшталт «найефективніша боротьба з тролінгом – ігнор». Це доречна позиція, проте її не можна і переоцінювати. Найкраще зберігати продуманий баланс, розуміючи діапазон ефективності і доречні межі кожного із способів реагування на проблему. Що ігнорувати? Доречно ігнорувати поодинокий негатив. Одноразові образливі повідомлення найкраще ігнорувати, часто в результаті цього кібербулінг на початковій стадії і зупиняється. Якщо ж реагувати на негативні коментарі, комунікація продовжується.

 Можливе блокування кривдника. Пауза в спілкуванні руйнує взаємопідсилювані автоматизми кібербулінгу, особливо якщо він мотивований втечею булерів від нудьги і не супроводжується булінгом у реальному житті. Коли ігнорувати не варто? Не дивлячись на те, що відправник Вам невідомий, якщо листи систематично містять загрози життю і здоров’ю, або порнографічні сюжети, то варто поставити до відома телефонного або Інтернет-провайдера, звернутися до відділу поліції. Якщо образлива інформація розміщена на сайті, варто зробити запит адміністратору щодо видалення цієї інформації. У цьому можуть допомогти

дорослі.



 3. Пам’ятайте, що віртуальні знайомі можуть бути не тими, за кого себе видають. Шахраї, зазвичай, дуже гарні психологи: представляючись одним з ваших давніх знайомих, вони дізнаються від вас конфіденційну інформацію, як, наприклад, адресу, коли у вас вдома нікого немає, з ким ви проживаєте, ваш майновий стан і т. д. з метою пограбування.

 4. Зустрічі у реальному житті із знайомими по Інтернет-спілкуванню не є дуже гарною ідеєю, оскільки люди можуть бути дуже різними у електронному спілкуванні і при реальній зустрічі. Якщо все ж таки це необхідно, то зустріч повинна відбуватися в громадському місті та у присутності друзів.

 5. Не розголошуйте нікому, навіть друзям, свої логіни і паролі до облікових записів електронної пошти, соціальних мереж тощо.

 6. Не відкривайте листи електронної пошти, файли або Web-сторінки, отримані від людей, яких ви не знаєте або не довіряєте – там можуть бути віруси.

7. Завжди перевіряйте правильність адреси веб-сайтів, на яких ви вводите конфіденційну інформацію. Часто шахрайські сайти мають адреси дуже схожі на адреси реальних веб-сайтів, але відрізняються, наприклад, однією літерою. Банки та сервіси електронної пошти не будуть починатись з http – тільки https!

 8. Пам`ятайте про небезпеку безкоштовного публічного Wi-Fi. Ці мережі можуть робити дані доступними.



**БУДЬТЕ ОБЕРЕЖНИМИ!**