КІБЕРБЕЗПЕКА

ЩО таке кібербезпека?

Кібербезпека — це захист цифрових систем, мереж та даних від кіберзагроз, таких як хакерські атаки, несанкціонований доступ та витік інформації. Вона охоплює широкий спектр заходів, від безпеки програмного забезпечення до навчання персоналу, щоб забезпечити надійний захист від кібератак.

ЯК ВБЕРЕГТИСЬ ВІД КІБЕРАТАК

Правило 1

Встановити на комп'ютер спеціалізовані антивірусні програмита оновлювати їх.

Правило 2

Не використовувати генератори паролів, краще придумати самотужки – з різними цифрами і знаками.

Правило 3

Не використовувати один пароль на всіх сайтах, додатках і пристроях.

Правило 4

Зберігати резервні копії особистих даних на пристроях без доступу до інтернету.

Правило 5

Завжди бути насторожі – ставити під сумнів підозрілі листи, посилання та програми.

ВИДИ КІБЕРАТАК

ФІШИНГ

Фішинг – це атака, яка в основному використовує електронну пошту як вектор та в обманний спосіб змушує людей завантажувати шкідливі програми на свої пристрої. Близько 75% організацій зіткнулися з фішингом у 2020 році.

АТАКИ ПРОГРАМ-ВИМАГАЧІВ

Програми-вимагачі (ransomware) – це шкідливе ПЗ, яке блокує доступ користувачів до їхнього програмного забезпечення і вимагає заплатити викуп. Зазвичай ransomware поширюється за допомогою спаму або соціальної інженерії.

ШКІДЛИВЕ ПЗ

Шкідливі програми зупиняють роботу пристроїв або значно уповільнюють їх. Програми-шпигуни, віруси, черв'яки, програми-вимагачі або програми-трояни – все це використовують кіберзлочинці. Шкідливе ПЗ потрапляє на пристрої через вкладення електронної пошти зі шкідливим кодом або через програми обміну файлами, які поширюють небезпечні матеріали, замасковані під музику або зображення.

ЩО ТАКЕ КІБЕРПОЛІЦІЯ

Кіберполіція (Департамент кіберполіції Національної поліції України) – це міжрегіональний підрозділ Національної поліції, який займається боротьбою з кіберзлочинністю. Її основні завдання: попередження, виявлення та припинення правопорушень, що вчиняються з використанням комп'ютерів та комп'ютерних мереж. Кіберполіція розслідує випадки кібернасильства, шахрайства, кібергрумінг, а також інші злочини, пов'язані з використанням Інтернету та інфомаційних технологій.

ВИДИ КІБЕРПОЛІЦІЇ

КІБЕР ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

Розслідування кіберзлочинів:

Кіберполіція розслідує такі злочини, як хакерські атаки, шахрайство в Інтернеті, розповсюдження шкідливого програмного забезпечення та інші злочини, пов'язані з використанням інформаційних технологій.

Запобігання кіберзлочинів:

Кіберполіція здійснює профілактичні заходи, щоб запобігти кіберзлочинам, інформує населення про загрози та надає рекомендації щодо кібербезпеки.

Інформування населення:

Кіберполіція проводить інформаційні кампанії, щоб підвищити рівень обізнаності населення щодо кібербезпеки та запобігання кіберзлочинів.

Систематизація кіберінцидентів:

Кіберполіція впроваджує програмні засоби для систематизації та аналізу кіберінцидентів, що дозволяє ефективніше боротися з кіберзлочинністю.

Співпраця з міжнародними партнерами:

Кіберполіція веде співпрацю з міжнародними організаціями та іншими країнами для обміну досвідом та боротьби з кіберзлочинністю.

ЯК ПОВІДОМИТИ ПРО КІБЕРЗЛОЧИН

Щоб повідомити про кіберзлочин, можна звернутися до Кіберполіції, зателефонувавши на лінію 102 або подавши електронне звернення через сайт https://ticket.cyberpolice.gov.ua. У разі загрози життю або здоров'ю, варто звернутися до найближчого відділку поліції або на лінію 102.

ЩО РОБИТИ КОЛИ НА ТЕБЕ ПРОВОДЯТЬ КІБЕР АТАКУ

Першочергово варто подбати про технічну складову, а саме заблокувати проведення будь-яких фінансових операцій, вимкнути пристрої, що піддалися кібератаці.

Далі варто попередити про атаку працівників компанії або державної установи, контрагентів, клієнтів. Важливо зберігати довіру та не вдаватися до паніки навіть у такі складні моменти. Всі ті, хто взаємодіє з об'єктом хакерської атаки, повинні знати про можливість розповсюдження їх персональних даних.

Звернення до правоохоронних органів. Наразі в Україні діє окремий орган Національної поліції (Кіберполіція), що спеціалізується на викритті, затриманні кібер-злочинців та вповноважений на проведення розшукової діяльності. Також необхідним є звернення із заявою до Оперативного центру реагування на кібер-інциденти, або ж до урядової команди реагування на комп'ютерні надзвичайні події, звернення можна надіслати на офіційну електронну пошту.

Проведення фіксації шкоди після хакерської атаки. Так як хакерська атака має в собі ознаки кримінального правопорушення, то згідно зі ст. 93 КПК потерпілий має право на збір доказів факту вчинення правопорушення. Одразу після початку хакерської атаки варто зафіксувати стан технічних пристроїв за допомогою фото-відеофіксації, задокументувати свідчення очевидців кібератаки, якщо це можливо зафіксувати факт втручання у систему.

Після подання заяви до правоохоронних органів протягом 24 годин має надійти витяг з реєстру досудових розслідувань, що стане підтвердженням того, що кримінальне провадження є відкритим, а саме перша його стадія - досудове розслідування.

В рамках досудового розслідування хакерської атаки, прокурор або слідчий проводять огляд місця події. Зазвичай така слідча дія проводиться за участю експертів, що мають відповідну кваліфікацію. Також можуть проводиться й інші заходи (допит свідків, призначення ряду експертиз), що допоможуть зібрати необхідні докази для досягнення мети розслідування.

Варто зазначити, якщо потерпілий від хакерської атаки вважає за потрібне проведення певних слідчих дій, то законодавством надається можливість їх ініціювання, шляхом подання клопотання (ст.220 КПК). Слідчий або прокурор повинні забезпечити присутність потерпілого при проведенні таких дій

ЧОМУ КІБЕРБЕЗПЕКА ВАЖЛИВА У СУЧАСНОМУ СВІТІ

Кібербезпека важлива у сучасному світі через широке поширення цифрових технологій та їхню залежність від Інтернету. Вона захищає від кібератак, крадіжки даних, шкідливого програмного забезпечення та інших загроз, які можуть мати серйозні наслідки для індивідів, компаній і навіть національної безпеки.

ЯК ЗАХИСТИТИ СВОЇ ДАННІ В КІБЕР ПРОСТОРІ?

Щоб захистити свої дані в кіберпросторі,

- використовуйте складні паролі,
- вмикайте двофакторну автентифікацію,
- будьте обережними з посиланнями та вкладеннями в електронній пошті,
- регулярно оновлюйте програмне забезпечення та використовуйте антивірус,
- а також робіть резервні копії даних.