ЗАТВЕРДЖУЮ
Начальник відділу оперативних чергових
підполковник служби цивільного захисту
Микола Джурбій
“___” _____ 2024 року

ПЛАН-КОНСПЕКТ
проведення заняття з навчальною групою № 15
01,02,03,04,08,09,10,11 січня 2024 року

Профільна підготовка

Відділ оперативних чергових МРЦ ШР ДСНС України

Тема: Електронна пошта в підрозділах ДСНС України та її використання.

Навчальна мета: Підвищення рівня знань та професійних якостей. особового складу.

Час: 45 хвилин.

Місце проведення: Робоче місце МРЦ ШР ДСНС України.

Навчально-матеріальне забезпечення: Самостійне навчання.

Нормативно-правові акти та література: 1. Наказ ДСНС №425 від 19.07.2019 року.

Порядок проведення заняття:

1. Організаційні заходи – 2 хв.:
   перевірка присутніх;
   оголошення теми і мети заняття.
2. Контроль знань – 5 хв.: перевірка засвоєння раніше пройденого Матеріалу.
3. Викладення матеріалу теми – 30 хв.

Питання та їх короткий зміст	Методичні вказівки
ЕЛЕКТРОННА ПОШТА Знайомлячись із новими людьми у справах чи побуті, ми все частіше питаємо не лише контактний номер телефону, а й адресу електронної пошти. Разом зі збільшенням попиту на цей зручний і безкоштовний засіб комунікації зростають і ризики від його втрати, чи ще гірше — заволодіння поштовою скринькою сторонніми особами. Мета цієї статті — простими словами пояснити доступні способи уникнення наслідків, пов'язаних із втратою «електронки». **1. Не використовуй приватну пошту для передачі службової інформації.** Ніколи не використовуй своєї особистої пошти (*Ukr.net, Gmail, Yahoo,* тощо) для передачі інформації, пов'язаної зі службою. Навіть якщо ця інформація неважлива чи не має грифа секретності, або навіть якщо хтось сказав, що це класна пошта, вона зашифрована, і взагалі «Не парся, я сто разів так робив», — НЕ РОБИ! Майже вся інформація, що передається через Інтернет, може бути перехоплена. Питання тільки в тому, наскільки вона добре захищена і скільки коштуватиме таке перехоплення (час, залучення спеціалістів). Методи і засоби перехоплення (часто автоматизовані) давно відомі і знаходяться в мережі, доступній будь-кому. Що вже казати про спецслужби сусідньої держави, які утримують цілі відділи висококваліфікованих спеціалістів для перехоплення та розшифровки даних. Навіть, здавалося б, нікому не потрібну перехоплену інформацію можна проаналізувати й отримати важливі розвіддані. Наприклад, елементарний акт списання дизпалива дасть змогу зорієнтуватися, скільки техніки в якому підрозділі, чи прогрівається вона, чи переміщується. Фотографія роздавальної відомості подушок і матраців може розкрити інформацію про кількісний — склад підрозділу. Кілька перехоплених повідомлень, пара фото в однокласниках і за «поребриком» уже знають, скільки в нас хворих, скільки БК завезли минулого тижня і навіть те, скільки людей поїде	Текст виділений курсивом дати під запис

на «Океан Ельзи» в Маріуполь. І буде вкрай неприємно, коли по дорозі на них чекатиме фугас...

Для вирішення подібних питань вже давно існує військова поштова скринька на *mil.gov.ua*. Вона надійна, і ти точно знаєш, що захищені сервери знаходяться на вузлі зв'язку, а не в сусідньому підвалі. Щоб її відкрити, просто підійди до зв'язківця, він допоможе. Крім цього, ЗС України за два роки розгорнули нові системи захищеної передачі даних (голос, електронна пошта, файлообмін і т.ін), які забезпечують надійну передачу, в тому числі й секретної інформації. Звісно, це вимагає додаткових дій — доведеться оформити супровідний лист і підписати його у командира, але що таке кілька хвилин паперової роботи в порівнянні зі збереженим життям?

Важливо. *Більшість антивірусів ідентифікує* ***Mail.ru Агент****, що самостійно встановлюється разом із однойменною поштою як потенційно небажане, шкідливе чи навіть шпигунське програмне забезпечення. Тому не варто користуватися їхніми продуктами. Як, зрештою, всім, що пов'язано з* ***.ru****.*

2. Розділяй поняття «службові» та «особисті» потреби під час використання електронної пошти.

Не використовуй свою поштову скриньку на *mil.gov.ua* (відкрита зв'язківцем твоя службова скринька) для реєстрації в соціальних мережах, форумах чи розважальних сайтах. Службова поштова скринька повинна використовуватися виключно у СЛУЖБОВИХ цілях, а не для листування з коханою. Для цього достатньо пошти на *Gmail, Yahoo* чи *Ukr.net.*

Використання своєї пошти на подібних ресурсах часто призводить до компрометації (злому або отримання доступу) чи зарахування в бази для подальшого збору інформації. Чи, може, ти думаєш, що в базі сайта *vkontakte.ru* дуже складно зробити налаштування пошуку профілів за поштою *mil.gov.ua*?

Іншим негативним аспектом є навантаження на канали зв'язку. В умовах проведення АТО в рази збільшилися обсяги інформації, що циркулює в наших телекомунікаційних системах. Відповідно, пересилання по військових каналах зв'язку (пошта з домену *mil.gov.ua* передається саме по них) красивих пейзажів Донеччини може створити не лише затримки в передачі важливої інформації, але й затримати виклик евакуатора для трьохсотих.

Для уникнення всього цього просто розділи поштових клієнтів на пристроях: службове листування — на АРМ або комп'ютері від армії, а особисте листування — з персонального ноутбука

чи комп’ютера.

3. Використовуй унікальні паролі під час кожної реєстрації нової поштової скриньки.

Використовувати однаковий пароль для різних скриньок, сервісів і реєстрацій досить зручно, його не забудеш з часом, не треба «тримати в голові» всі ці назви, цифри, комбінації. І найголовніше — не треба витрачати час, щоб зайти на скайп чи у фейсбук. Незважаючи на всі очевидні переваги, така практика має один суттєвий недолік — це ставить під загрозу всі облікові записи чи реєстрації з однаковим паролем.

Для прикладу типовий сценарій. При реєстрації на інтернет-форумі необхідно ввести свою електронну пошту і придумати пароль до нового акаунту (обліковий запис) на форумі. Користувач ввів свою електронну адресу, яка буде використана, як ім’я нового акаунту, пароль — «улюблений», який використовується для всього: доступу до пошти, яку він щойно надав, доступу до онлайн-банкінгу, соціальних мереж тощо. Тепер в адміністратора форуму (або хакера, який перехопив цей пароль) є електронна адреса і ймовірний пароль до неї. Зайшовши на цю адресу з паролем, зловмисник отримує доступ до всіх інтернет-сервісів, які зареєстровані на цю скриньку. Жертвами такого підходу щодня стають тисячі користувачів Інтернету.

Щоб самому не поповнити ряди «хакнутих» жителів Інтернету, при кожній реєстрації використовуй різні паролі або, щонайменше, пароль, відмінний від пароля електронної пошти. Щоб не заплутатися чи не забути, можна записувати їх та зберігати в надійному місці (але не на комп’ютері у файлі «Пароль!!!») або використовувати якусь зрозумілу схему створення нових паролів.

Важливо. *Власна схема створення паролів є надійним способом захистити свої дані. Як варіант, придумуєш сталу комбінацію, що легко запам’ятовується, і під час кожної реєстрації просто доповнюєш цю комбінацію назвою сайта, на який реєструєшся, чи символами, датами.*

4. Тримай пароль у таємниці й нікому його не повідомляй.

Останнім часом для отримання важливої інформації зловмисники все частіше користуються прийомами так званої соціальної інженерії. Якщо до тебе пишуть чи телефонують і дуже переконливо пояснюють, навіщо їм треба та чи інша інформація про твою пошту, особливо пароль, тобі варто задуматися.

Інший популярний спосіб витягнути твої дані – це відправка

листів з посиланням на сайт, де необхідно повторно ввести ім'я користувача і пароль. Такі листи завжди виглядають дуже переконливо, оформлені відповідним чином і навіть містять персональні дані, відомі тільки справжньому адміністратору. Це все створює враження легітимності запиту пароля. Для проведення такої атаки використовуються різноманітні психологічні прийоми. Це можуть бути прохання про допомогу, спільні знайомі чи навіть бажання приємної дівчини поспілкуватися з солдатом на передовій. Може навіть прийти попередження про відключення електронної пошти або її зараження, для підтвердження особистості необхідно ввести пароль. У листі надається посилання на сайт, який виглядає точнісінько як веб-пошта, єдина різниця, що введені дані відправляються зловмиснику.

Щоб цього не трапилося, НІКОЛИ і НІКОМУ, ні під яким приводом не повідомляй жодної інформації стосовно своєї поштової скриньки, жоден адміністратор ні в якому разі не питатиме жодної інформації (окрім власне адреси цієї скриньки). Всю інформацію, що може їм знадобитися, вони вже отримали під час твоєї реєстрації. У разі отримання такого запиту на службову пошту необхідно повідомити зв'язківця або помічника командира підрозділу із захисту інформації. Якщо подібний лист отримано на приватну пошту — повідом технічну підтримку поштового сервісу і надішли копію отриманого листа. Таким чином вони зможуть оперативно попередити інших користувачів і швидко звести зусилля противника нанівець.

Не потрібно додаткових пояснень, щоб зрозуміти, що пароль, записаний на клаптику паперу і приклеєний до монітора, не є надійним способом збереження паролів. Ми ж не залишаємо ключі від дому на гачечку біля вхідних дверей.

Важливо. *Більшість мережевих сервісів, у тому числі й електронна пошта, побудовані таким чином, що адміністратор сервісу не має доступу до (читай — не повинен знати) паролів користувачів. НІКОЛИ не передавай пароль, незважаючи навіть на переконливість запиту.*

5. Використовуй лише стійкі паролі.

Не використовуй свою дату народження чи когось із близьких як пароль до своєї пошти. Такий пароль можна досить швидко вгадати. Використання «слабкого» паролю на зразок «parol12345678» призводить до злому пошти, і це справа часу.

Щоб не забути свій пароль, користувачі електронної пошти часто використовують імена чи дати народження близьких. Звісно,

що такий пароль ніколи не забудеш, але, водночас, підібрати його дуже легко. Для цього достатньо дізнатися імена та дати народження власника пошти, яку необхідно зламати, а також дані його близьких. Такі дані не так складно здобути, наприклад, більшість користувачів «залюбки» надають свої персональні дані в соціальних мережах, там же можна знайти дані близьких і родичів, уподобання та іншу інформацію, корисну при підборі пароля. Перебір можливих комбінацій навіть уручну займе не так багато часу, а за наявності базових навичок програмування цей час суттєво зменшиться.

Використання коротких паролів або паролів, складених з використанням загальновживаних слів, значно спрощує життя охочим отримати доступ до чужих поштових скриньок. Для підбору таких паролів є спеціальні словники, в яких містяться найбільш уживані паролі. Напевне, кожен з нас хоч раз та використовував пароль «1111», «87654321», «qwerty123» або щось подібне. Підбір саме такого пароля спеціальними програмами займає кілька секунд. Якщо на поштовому сервісі встановлено обмеження на кількість спроб уведення пароля, час підбору хоч і збільшується, та все одно це справа часу. Пароль «12345678» входить до п'ятірки найбільш уживаних паролів у світі, його підбір займає кілька наносекунд. Якщо ти використовуєш подібний пароль — вважай, що твоя пошта не має пароля взагалі!

Також варто знати, що існують програми, які автоматично проводять аналіз сторінок «цілі» в соціальних мережах, збираючи персональну інформацію про його/її уподобання, близьких. На основі такої інформації формується персоналізований словник імовірних паролів, що значно прискорює отримання несанкціонованого доступу до скриньки.

Тому використовуй стійкі паролі довжиною не менше 10 символів, які містять великі й малі літери, цифри та спеціальні символи (!@#_$+%=^&-*). Щоб зробити такий стійкий пароль легким для запам'ятовування, можна використовувати цілі фрази та власну систему генерації паролів, як уже зазначалося. Наприклад: Meni_P0d0baetsa_Sp0rt (основа: Мені Подобається Спорт, замість букви «О» — нулі, між словами — підкреслення). Такий пароль відповідає всім згаданим вимогам, його легко запам'ятати, підбір усіх можливих комбінацій для такого пароля займатиме кілька десятків років. Використання ще кількох спецсимволів може збільшити складність підбору в кілька тисяч разів.

Важливо. *У разі злому поштової скриньки власник навряд чи про це дізнається. Противник буде використовувати як ще одне*

джерело отримання інформації чи розсилки дезінформації. Тому те, що ти користуєшся поштою і «все нормально», не значить, що цю пошту «не моніторять».

6. Не натискай на посилання і прикріплені файли, отримані в листі.

Одним з найефективніших шляхів розповсюдження комп'ютерних вірусів є розсилка їх по електронній пошті. Ні, це не офіційні розсилки хакерських груп з проханням завантажити їх новий вірус і поділитися з ними важливою інформацією. Це листи, що містять якусь інтригуючу або цікаву інформацію, споріднену з твоїм видом діяльності чи інтересами — гарні фото (не виключено що й твої, викрадені напередодні), посилання на відео, сайт з новинами про демобілізацію, словом те, що спонукає клікнути на посилання. Небезпека полягає в тому, що досить єдиного кліку для прихованої інсталяції шпигунського програмного забезпечення або запуску операцій на вже інфікованому пристрої, наприклад, переадресації всієї кореспонденції зловмиснику.

Тому якщо ти отримав листа, у якому містяться посилання на інші сайти, прикріплені фотографії чи інші файли — ні в якому разі не переходь за цими посиланнями і не намагайся переглянути завантажені файли. Звісно, якщо ти знаєш, що зараз маєш отримати архів з фото чи відео, то все добре. Але якщо раптом отримуєш листа з документом «Нарахування бойових» та ще й з адреси *financy56ombr_mil_gov_ua.**mojdnr.com***, то варто задуматися. Найімовірніше, це привіт, відправлений з «деенерії» (*moj.dnr.com*), хоча так схоже на *mil.gov.ua* і так хочеться почитати про нарахування премій.

Протидія такого роду атакам досить проста. Найперше, це не відкривай нічого, якщо стовідсотково не впевнений. Якщо маєш сумніви щодо автора чи вмісту листа, зв'яжися з відправником іншими засобами зв'язку та уточни час відправлення, назву та розмір відправленого файла (назву посилання, кількість фото тощо). Якщо щось не збігається, НЕГАЙНО надай доповідь командиру і розкажи зв'язківцю або, якщо є, помічнику командира із захиту інформації та кібербезпеки. Такі атаки, зазвичай, здійснюються масованими розсилками подібних листів, тому оперативність реагування відіграє визначальну роль у протидії зловмисникам.

Важливо. *Найвідомішим випадком використання цієї техніки стало інфікування у 2000 році мільйонів комп'ютерів вірусом I_LOVE_YOU. Після відкриття такого «листа кохання» вірус пошкоджував файли на комп'ютері й автоматично розсилався*

далі, використовуючи адресну книгу інфікованого комп'ютера. Тому навіть отримання листа із вкладеннями чи посиланнями від товариша чи колеги по роботі не означає, що лист безпечний і не містить вірусів. РОЗКАЖИ ТОВАРИШАМ, ПОЯСНИ РІДНИМ ТА БЛИЗЬКИМ!!!	

4. Закріплення вивченого матеріалу – 2 хв.
5. Підбиття підсумків - 3 хв.: зазначення питань, що потребують підвищеної уваги; оголошення оцінки; відповіді на запитання.

Конспект-лекцію склав:
Оперативний черговий
підполковник служби цивільного захисту Михайло КУКЛА

«__»_____2023 р.