Безпека в соціальних мережах – етика поведінки в інтернеті. Як уникнути атак на вашу віртуальну особистість – у порадах експертів.

Соціалізація та соціальні мережі все глибше проникають у життя користувачів, і все більше місце в реальному житті займає віртуальне спілкування. Сьогодні простіше розіслати запрошення друзям на День народження через Facebook, аніж запросити їх особисто, обдзвонити телефоном або розіслати запрошення поштою.

Саме через популярність та глибину проникнення в наше життя зловмисники все більше й більше звертають увагу на те, як і про що ми спілкуємося в соцмережах. Ми хочемо ділитися зі своїми друзями новинами про нову покупку, про майбутню відпустку з усією сім'єю, про отриману премію. Але якщо хтось просто порадіє за вас (або позаздрить), то хтось може задуматися зовсім про інше: «Ага! Тут є чим поживитися!». Нижче наведемо кілька правил і простих порад, які допоможуть уникнути атак на вашу віртуальну особистість.

1. Вибір соціальної мережі. При реєстрації в новій соціальній мережі прочитайте її політику конфіденційності уважніше, а не просто ставте галочку «я згоден (на)». Практично всі соцмережі можуть збирати персональні дані про вас, про сайти, які ви відвідуєте, про ваші інтереси та вподобання. Основна мета збирання таких даних – розширення аудиторії соцмережі й пропозиція таргетованої реклами своїм користувачам. З одного боку, в цьому немає нічого поганого, адже соцмережі мають на чомусь заробляти. З іншого – вони можуть заробляти на продажу ваших конфіденційних даних іншим зацікавленим компаніям. У політиці конфіденційності і в угоді користувача повинно бути чітко прописано, які саме дані соцмережа збирає про вас, як зберігає, як обробляє й кому може передавати, а кому – ні. Так само слід звернути увагу на наявні засоби щодо контролю за безпекою вашого профілю, чи є можливість відновлення пароля, чи є прив'язка до мобільного телефону, за яким протоколом здійснюється передача даних, відкритому або шифрованому, чи можна налаштувати приватність своєї сторінки та обмежити її перегляд повністю або частково. Варто звернути увагу й на те, чи може соцмережа взаємодіяти з вашим комп'ютером або іншими

сервісами, окрім як через браузер. Деякі соцмережі можуть просити надати вашу адресу електронної пошти та пароль до неї, щоби просканувати вашу адресну книгу.

Або ж попросять скопіювати адресну книгу, розташовану на локальному комп'ютері. Використовуючи цю інформацію, соцмережі можуть розсилати запрошення приєднатися до соцмережі вашим друзям від вашого імені. Але достовірно дізнатися, як саме ця інформація буде використовуватися, можна тільки уважно прочитавши угоду користувача (й то не завжди).

З іншого боку, треба з'ясувати, що соцмережа дозволяє завантажувати в неї. Дізнайтеся, чи існує на сайті контроль контенту, який публікується його користувачами, чи можна завантажувати будь-яку музику й відео, чи є обмеження за віковим контентом (наприклад, тільки 16+ або 18+). До сайтів, де ви залишаєте свої конфіденційні дані, варто підходити так само серйозно, як і до сайтів, на яких ви розраховуєтеся кредитною карткою. А іноді навіть і суворіше.

2. Одна чи кілька? «Вконтакте», «Одноклассники», Twitter, Instagram, LinkedIn, Google+, Facebook – у світі більше 200 великих соціальних мереж, 15 мають більше 100 мільйонів активних користувачів, більше 60 з них російськомовні. Невже потрібно реєструватися в усіх? Відкиньмо безліч тематичних платформ, не українсько- та російськомовних, ті, де немає ваших друзів, і ті, дизайн яких вам не сподобався. Залишиться близько п'яти – семи. Але навіть 5 може бути багато.

По-перше, обсяг інформації, яку буде необхідно обробляти. Якщо у вас якась радісна подія, опублікувати і продублювати її потрібно буде в п'яти різних місцях. У кожній мережі ви, безсумнівно, знайдете багато друзів, які будуть вам писати, але чи будете ви встигати відповідати всім? Ні, не так – ВСІМ?! Адже якщо обсяг вашої інформації зростає в арифметичній прогресії, то інформація, що генерується друзями – в геометричній. Ви просто не встигнете обробити її фізично. Вам доведеться або жертвувати роботою / сім'єю / сном, або «друзями» – хтось рано чи пізно почне ображатися.

По-друге, контроль інформації. Не завжди хочеться, щоб колеги знали про ваші захоплення, а друзі – де ви працюєте. Маючи

багато акаунтів, легко заплутатися, і, врешті -решт, ви щось не те «ляпнете», що негативно позначиться на вашій репутації.

По-третє, чим більше у вас акаунтів, тим складніше керувати аутентифікаційними даними – великий ризик втратити той чи інший пароль. І з іншого боку, зловмисникові, який зламав один із акаунтів, буде набагато простіше зламати й інші. Тому найкраще вибрати одну із соцмереж, яка найбільше сподобалася, і використовувати всі її можливості на 100%. Та якщо ви вирішили реєструвати в декількох мережах, скористайтеся простими порадами:

- розділіть їх за напрямами й тематикою. Наприклад, в LinkedIn спілкуйтеся тільки з колегами, в «Facebook» – тільки родичами, а «Instagram» залиште друзям;

- логіни на кожен акаунт повинні бути різними, а паролі складними. Щоб не забути їх і не вводити вручну, скористайтеся менеджером паролів;

- у кожній соцмережі є система відновлення паролю за допомогою альтернативного поштової скриньки або мобільного телефону. Зробіть різні скриньки для кожної соцмережі, інакше, зламавши пошту або отримавши вашу сім-карту, зловмисник матиме доступ до всіх акаунтів.

3. Заповнення профілю в мережі і його налаштування. На першому етапі соцмережа попросить вас заповнити ваш профіль. Які дані необхідні? Звісно ж, прізвище, ім'я, по батькові, рік народження. Де народилися, де вчилися. Фото, друзі, родина. А що ви вказуєте в полі «пароль» і «контрольне запитання»? Свій день народження і дівоче прізвище матері? Так вони ж у вас на головній сторінці в профілі опубліковані! Фактично ви самі віддали їх зловмисникові. Які ще є стандартні контрольні питання? Кличка улюбленої тварини? Улюблене чоловіче (жіноче) ім'я? Все це легко знайти у вашому профілі, якщо неуважно поставитися до цінності інформації, яку ви публікуєте. Тому пароль повинен бути досить складним, не містити жодних персональних даних, на зразок імені або дня народження, і відповідь на контрольне запитання повинні знати тільки ви. Також при заповненні профілю особливу увагу слід приділити налаштуванням приватності – хто може бачити ваші фото, хто

може їх коментувати, хто має доступ до вашої інформації – будь-хто чи тільки ваші друзі?

Також рекомендується регулярно перевіряти ці налаштування: соцмережі можуть змінити їх без вашого відома й тоді все, що ви довіряли лише друзям, стане загальнодоступним. Для підвищення рівня безпеки своїх користувачів соцмережі постійно вдосконалюють засоби безпеки і всіляко допомагають користувачам – це і детально прописані розділи в рубриці «допомога», інструкції при заповненні профілю, і різні спільноти. Та й техпідтримка, зрештою, – не ігноруйте всю пропоновану вам допомогу. Уважно вивчіть усі можливості – це і прив'язка до мобільного телефону, і «довірені друзі», і GeoIP, і HTTPS, і багато інших способів – користуйтеся.

4. Шлях до рідного дому. Коли ви створили всі необхідні акаунти, збережіть посилання на ваші сторінки в обраному, і при переході на сайт користуйтеся тільки ними. Так ви будете впевнені, що ввели адресу правильно і не потрапите на фішингові сайти, випадково або якщо вас туди заманили. Коли вам прийшло сповіщення про нове повідомлення, або запрошення друга, або лист від «адміністрації» ресурсу – не натискайте на посилання в листі, а зайдіть в свій акаунт у звичний і перевірений спосіб. Так ви уникнете фішингових і багатьох інших атак.

5. Скажи мені, хто твій друг. Безумовно, друзі й послідовники – це добре. Але хто вони? Чи ті вони, за кого себе видають, і чи це люди взагалі, чи роботи? Якщо ви налаштували доступ до своєї сторінки лише для друзів, подумайте, навіщо людина просить додати себе в друзі? Поспілкуватися чи отримати доступ до закритої частини профілю? Чимало шахраїв використовують фальшиві акаунти, щоб побільше дізнатися про вас. І наступного разу, коли вона напише й надішле посилання, ви будете їй довіряти, адже це ваш «друг»! Навіть якщо до вас постукала людина, котру ви знаєте в реальному житті, не поспішайте її додавати, зв'яжіться з нею по телефону, електронною поштою чи будь-яким іншим перевіреним каналом зв'язку й запитайте, чи дійсно то вона до вас звернулася. Або, якщо це неможливо, запитайте в співрозмовника щось таке, про що може знати тільки ваш друг.

6. Я є тим, що я ~~їм~~ пишу. Коли незнайома людина дивиться ваш профіль, у неї складається враження про вас з огляду не на те, що є насправді, а на те, що ви захотіли показати. А побачити ваш профіль може будь-хто. Навіть так: ХТОСЬ! Наприклад, молодий хлопець виклав фотозвіт про похід у крутий бар або заміський клуб. Що подумають друзі: «О! Та ти крутий!! Молодца!». Що подумають батьки: «Е-е, здається в той день він казав, що всю ніч учитиме математику?». Що подумає його дівчина: «Це що там за блондинка праворуч??!!». Що подумають в університеті: «Замість учити математику цей двієчник розважається». Що подумають зловмисники: «Ага, в цього молодого гульвіси і його батьків є гроші». Що через 10 років подумає його потенційний роботодавець: «Ні, ми не можемо взяти такого безвідповідального гуляку, незважаючи на те, що він відмінний фахівець і має хороші рекомендації». Точно так само з іншою інформацією – ви ніколи не знаєте, де ця інформація може з'явитися і яку роль зіграє в майбутньому.

7. Сміттєвий бак не працює. Якщо ви все ж усвідомлюєте помилки минулого і вирішите видалити всю інформацію про свою бурхливу молодість, навряд чи це вийде. Соціальні мережі не зацікавлені в тому, щоб ви їх покинули, й максимально ускладнять процес видалення акаунта. Якщо ж ви знайшли заповітну червону кнопку, не поспішайте радіти. Деякі соцмережі зберігають інформацію про вас навіть при віддаленому обліковому записі (уважно читайте угоду користувача). Якщо у вас багато акаунтів у різних соцмережах, ви просто забудете, що й коли публікували, й видалите не все. Так само цю інформацію може зберегти ваш співбесідник у себе в профілі, або взагалі на домашньому комп'ютері, тоді у вас не буде доступу до неї. Якщо ваші фото з вечірки справді були «бомбою!!», ваші друзі викладуть їх у себе в профілі, а потім їхні друзі – в себе, й так далі – цієї лавини не зупинити...

8. Спілкування без конкретики. Обдумуйте, що ви публікуєте на своїй сторінці соцмереж, на форумах; що пишете, коли спілкуєтеся в месенджерах або використовуєте будь-які інші засоби для спілкування. Це важливо, оскільки допоможе уникнути втрати ваших особистих даних, а також дозволить запобігти будь-якій іншій шкідливій діяльності, яка може вам погрожувати. Наприклад, дані про ваше повне ім'я, дівоче прізвище матері,

номери ваших телефонів, адреси, дата народження тощо можуть нести потенційну небезпеку, адже ви не можете бути впевнені, що дані не стануть загальнодоступними. При листуванні не використовуйте конкретних даних, намагайтеся застосовувати тільки загальні формулювання, так зловмисник не зможе скористатися вашою інформацією проти вас. Коли робите фотографії, звертайте увагу на задній план: номери машин, адресу будинку чи ресторану, де ви постійно обідаєте, або місце розташування сигналізації в будинку. Вимкніть GPS-мітки в смартфоні або фотоапараті, інакше зловмисники знатимуть ваш розпорядок дня з точністю до хвилин.

9. І ти, Брут? В інтернеті ваш найкращий друг – скептицизм. Хоча в соціальних мережах тонни корисної інформації, ставтеся до неї з неабиякою часткою недовіри – людям властиво брехати. Хочуть перебільшити свої заслуги або ж отримати якусь пряму вигоду – не важливо. Це можуть бути зловмисники, які пишуть вам від імені чарівної блондинки, щоб вивідати номер кредитки. А можуть бути люди, що хочуть підняти свою самооцінку шляхом образи і провокування інших людей. Не годуйте тролів – не піддавайтеся на провокації з боку неадекватних користувачів (але й не уподібнюйтеся до них). Не втрачайте пильності за жодних умов. Суть у тому, що інтернет дозволяє представитися ким завгодно, хоч Папою Римським. Тому намагайтеся перевіряти інформацію, яку вам пропонують; з іншого боку, ніколи не діліться своєю персональною інформацією, яку може бути використано проти вас чи ваших близьких. Ніколи не відкривайте посилання, не перевіривши їх, навіть якщо їх надіслали друзі, хакери можуть зламати їхній обліковий запис і розсилати спам і фішингові посилання від імені людей, яким ви довіряєте. Перевірте посилання антивірусом, перш ніж відкрити.

Будьте медіаграмотними і нехай зловмисники Вам на просторах інтернету не трапляються!