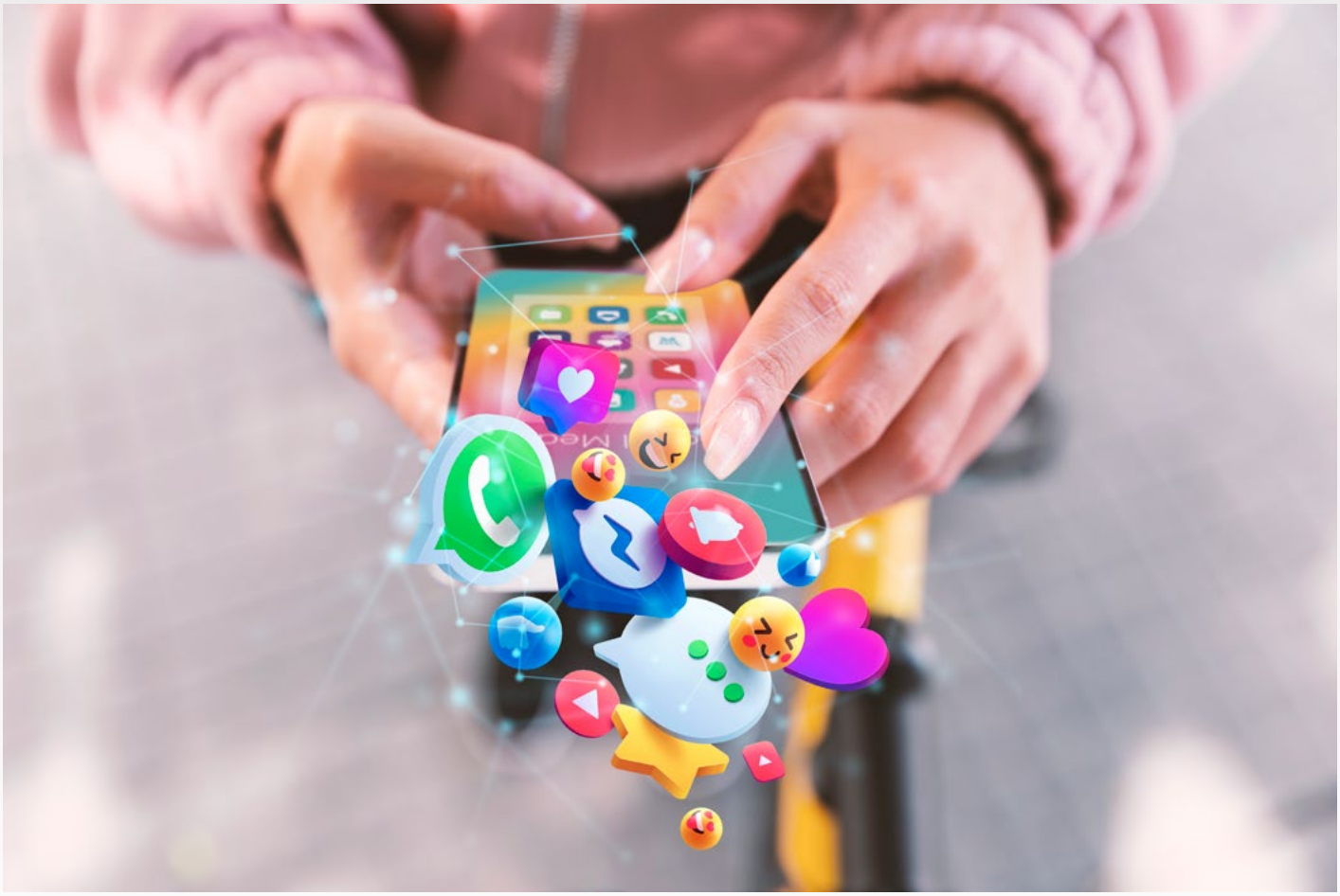
fundacja instytut
CYBERBEZPIECZEŃSTWA

Chroń swój wizerunek w sieci



Mówi się, że jak cię widzą, tak cię piszą. Nie sposób się z tym nie zgodzić. Pierwsze wrażenie możemy zrobić na kimś tylko raz, a cały proces trwa zaledwie kilka sekund. W dobie rozwoju technologicznego nasz wizerunek również znalazł się w sieci. Powiedzieć, że został tam przeniesiony, to jednak za dużo. Wciąż przecież poznajemy nowych ludzi, chodzimy na spotkania, dbamy o nasz wygląd i odpowiednie zachowanie w świecie realnym. Ale dbałość o nasz tradycyjny wizerunek jest zupełnie inna od jego kreacji w internecie. W związku z tym czyhają na nas inne zagrożenia, z którymi musimy się mierzyć, by stworzyć i zachować pożądany wizerunek w sieci.

Czym jest wizerunek w sieci?

Wizerunek w internecie to, najogólniej rzecz biorąc, wszystko to, po czym można nas zidentyfikować. Składają się na niego udostępnione przez nas zdjęcia, posty, polubienia stron i postów innych osób, nasze komentarze, sposób wyrażania się, obserwowane przez nas strony, wydarzenia, w których bierzemy udział, i treści, w których oznaczają nas znajomi. W internecie nic nie ginie. Nawet materiały opublikowane przez nas wiele lat temu i usunięte już z naszego konta mogą mieć wpływ na nasz wizerunek. Nie mamy gwarancji, że nikt nie zdążył ich skopiować. Ślad po nich pozostanie też np. na serwerach wyszukiwarek i jest możliwy do odzyskania. Z kreowaniem naszego wizerunku w sieci kojarzą nam się głównie portale społecznościowe – Facebook, Instagram, LinkedIn, BeReal i wiele innych. Bardzo słusznie! To właśnie tam, w 2022 roku, przeciętny polski internauta spędzał około dwie godziny na dobę! Oprócz mediów społecznościowych, w których koncentrują się działania wizerunkowe, należy zwrócić uwagę na nasze zachowanie na forach tematycznych. Mimo że jesteśmy tam anonimowi (wyświetla się tylko nasz nick), nie wypada wyrażać się nieuprzejmie czy wyśmiewać innych użytkowników. W ten sposób nabieramy złych nawyków, które mogą rzutować na nasze późniejsze kształtowanie wizerunku. Co więcej, nie mamy pewności, że osoba, w stosunku do której źle się zachowaliśmy, myśląc, że jesteśmy anonimowi, nie pozna naszej prawdziwej tożsamości, chociażby przez wspólnych znajomych. Jeśli dojdzie do naruszenia prawa, funkcjonariusze policji również nie będą mieli najmniejszych kłopotów z ustaleniem naszej tożsamości.

Dlaczego musimy dbać o swój wizerunek w internecie?

Odpowiedź wydaje się oczywista. Chociaż funkcjonujemy w dwóch rzeczywistościach, realnej i wirtualnej, to nadszarpnięcie wizerunku w jednej z nich może przełożyć się na pogorszenie go w drugiej. Media społecznościowe bywają pierwszym miejscem, z którego ludzie dowiadują się o naszym istnieniu, więc nasz profil odpowiada za pierwsze wrażenie i wstępną opinię o nas. W obecnych czasach, nawet starając się

o nową pracę, musimy liczyć się z tym, że rekruter sprawdzi nasze profile w mediach społecznościowych. Dbałość o dobre zdjęcia, udostępnianie postów związanych z naszymi zainteresowaniami, umiejętnościami i osiągnięciami może wpłynąć na postrzeganie nas jako potencjalnie dobrych pracowników. Jeśli to Ty jesteś przedsiębiorcą i szukasz wspólników lub klientów, zapewne także sprawdzisz ich najpierw w internecie, a potem zaoferujesz swoje produkty czy usługi. Wizerunek on-line ma wpływ na nasze relacje społeczne. To, co udostępniamy, jak wypowiadamy się na niektóre tematy, rzutuje na nasze kontakty z przyjaciółmi, rodziną i innymi ludźmi. Negatywne treści oraz kontrowersyjne opinie mogą źle wpłynąć na relacje interpersonalne. Informacje publikowane na naszych profilach mają też związek z naszym bezpieczeństwie w internecie. Podczas zakladania profilu nie podawajmy wielu osobistych informacji lub zastrzegajmy do nich dostęp. Może nas to uchronić przed cyberatakami, szantażem i innymi negatywnymi skutkami.

Zagrożenia dla naszego wizerunku w internecie

Paradoksalnie, dużym zagrożeniem dla naszego wizerunku jesteśmy my sami. Udostępniamy nieodpowiednie treści i niekorzystne, z pozoru zabawne, zdjęcia. Z własnej woli lub sprowokowani wyrażamy się nieuprzejmie lub w niekulturalny sposób manifestujemy swój pogląd na jakąś sprawę. Czasami nie do końca świadomi sprowadzamy na siebie jakieś zagrożenie. Wiele osób nie zdaje sobie sprawy z tego, jak istotne informacje udostępnia w internecie. Upublicznienie danych osobowych czy osobistych informacji może zszargać naszą reputację na bardzo długi czas i narazić nas na inne konsekwencje, jak kradzież danych. Za nasz wizerunek odpowiadamy głównie my sami, ale często do jego poprawy lub niestety pogorszenia mogą przyczynić się nasi znajomi, publikując niewygodne dla nas treści, lub zdjęcia, na których wyszliśmy mało korzystnie. Takim sytuacjom najlepiej zapobiegać, chociażby przez odpowiednie ustawienia preferencji na naszym profilu. Warto ustawić powiadomienia o tym, że ktoś oznaczył nas w nowych treściach. Jeszcze lepszym rozwiązaniem jest zablokowanie tej opcji, lub – jeśli jest to możliwe – pozwolenie na dodanie oznaczenia tylko po naszej wcze-

śniejszej akceptacji. Pamiętajmy, że działa to też w drugą stronę. Jeśli jakiś materiał może negatywnie wpłynąć na wizerunek innych – nie udostępniajmy go! Zagrożenia pochodzące zupełnie z zewnątrz, które mogą wyrządzić nam dużo szkody, to przejęcia przez oszustów kont w mediach społecznościowych. Kradzież naszej tożsamości pociąga za sobą poważne konsekwencje, przed którymi nie ochronimy się jedynie ostrożnym dobieraniem publikowanych treści.

Jak i dlaczego ktoś kradnie nasz profil?

Oszuści przejmują nasze konta z wielu powodów. Po pierwsze, mogą to robić z pobudek finansowych. Przestępca włamuje się na nasz profil, po czym rozsyła do naszych znajomych wiadomości z prośbą o przelew, zwykle na małe kwoty, lub żąda od nas okupu za zwrot dostępu do konta. Po drugie, może to być zwykła ciekawość, złośliwość lub chęć dotarcia do informacji. Chociaż w Polsce uzyskanie dostępu do systemów informatycznych i informacji nieprzewidzianych dla nas jest penalizowane (art. 267 Kodeksu karnego), nie do końca odstrasza to potencjalnych cyberprzestępców, którzy by osiągnąć swój cel, stosują różne metody. Wśród nich można wymienić prowadzenie fałszywych witryn internetowych. Użytkownik logujący się na nieprawdziwej stronie, łudząco przypominającej konkretny portal społecznościowy,

nieświadomie podaje oszustom swój login i hasło. Takie działanie przestępcy mogą poprzedzać kampaniami spamowymi, co polega na wcześniejszym wysyłaniu wiadomości e-mail, rzekomo od administratora używanego przez nas portalu, z prośbą o logowanie w określonym celu. Złodziej może posłużyć się narzędziem takim jak keylogging (rejestracja klawiszy). Jest to złośliwe oprogramowanie, które śledzi i rejestruje każde naciśnięcie klawisza, w tym dane logowania i przekazuje wciśnięte przez nas kombinacje do komputera oszusta. Nasze hasło, jeśli jest słabe i takie samo jak do innych kont, może wyciec z innego źródła bądź po prostu zostać odgadnięte. Jeżeli oszust przejmie konto, w naszym imieniu mogą być wysyłane nie tylko wspomniane prośby o przelewy, lecz także publikowane fałszywe zdjęcia i wpisy. Przestępca może w naszym imieniu rozpocząć rozmowę z naszymi znajomymi, rodziną lub nawet skontaktować się z naszym szefem czy wykładowcą na uczelni, by rozsyłać obraźliwe treści i negatywnie wpłynąć na naszą reputację, a nawet wywołać konsekwencje prawne. Z naszego konta mogą być prowadzone ataki phishingowe, mające na celu wyłudzenie danych osobowych lub finansowych od znajomych. Oszust może też zmienić wszystkie dane na koncie lub zupełnie je zlikwidować.

Moje konto zostało skradzione. I co teraz?

Jeśli zauważyłeś lub zostałeś poinformowany o dziwnej aktywności na twoim koncie, lub dostałeś mail alarmujący o logowaniu z innego urządzenia bądź zmianie hasła – najpewniej ktoś właśnie przejmuje twoją internetową tożsamość! Kroki, które możemy podjąć, zależą od tego, czy wciąż jesteśmy zalogowani na jakimś urządzeniu i mamy dostęp do naszego konta. Jeśli tak, sprawdźmy w ustawieniach, jaki adres e-mail i numer telefonu jest przypisany do naszego profilu. Jeśli zauważymy tam obce dane, należy je natychmiast usunąć. Przestępcy najpewniej w ten sposób chcą zmienić hasło i odebrać nam dostęp do konta. Jeśli portal umożliwia sprawdzenie ostatnich logowań, koniecznie to zrób! W przypadku gdy zauważysz logowania z obcych urządzeń i lokalizacji, wyloguj te sesje. Następnie zmień hasło do swojego portalu społecznościowego. Sytuacja komplikuje się, jeśli przestępcy zdążyli już całkowicie

przejąć nasz profil i mimo poprawnych danych logowania system odrzuca nasze hasło. Wtedy należy podjąć próbę zmiany za pomocą opcji „nie pamiętam hasła". Jeżeli ta metoda się nie powiedzie, zgłoś sprawę do centrum pomocy. Sposób zgłaszania nieco różni się w zależności od portalu społecznościowego, ale jest dostępny na każdym z nich. Na przykład na Facebooku możesz to zrobić, prosząc o pomoc znajomego. Zalogujcie się na jego konto i wejdźcie na skradziony profil, rozwińcie menu, znajdźcie zakładkę „uzyskaj wsparcie lub zgłoś materiały" i zgłoście kradzież konta, postępując dalej zgodnie z instrukcjami Facebooka. Poinformuj swoich znajomych a przejęciu konta i ostrzeż ich, by nie wchodzili w żadne interakcje z oszustem. Dla pewności możemy zastrzec nasz dowód osobisty i kartę płatniczą. Jeśli przestępca wykonał jakieś działania, podszywając się pod nas, sprawę powinniśmy zgłosić na policję. Zgłoszenie ochroni nas lub przynajmniej złagodzi możliwe konsekwencje utraty tożsamości.

Lepiej zapobiegać niż leczyć

Dbałość o bezpieczeństwo naszego wizerunku w internecie to proces ciągły, rozpoczynający się już na etapie tworzenia profilu. Rejestrując się na portalu społecznościowym, ustal silne hasło, odmienne od tych, którymi logujesz się na inne strony. Regularnie zmieniaj swoje hasła. Dla dodatkowego zabezpieczenia włącz weryfikację dwuetapową. Bądź wyczulony na ataki phishingowe. Nigdy nie klikaj w podejrzane linki ani nie podawaj danych logowania w odpowiedzi na wiadomości otrzymane przez e-mail czy komunikator typu Messenger. Regularnie monitoruj aktywność swojego konta, aby szybko zareagować na pojawiające się nieprawidłowości. Warto włączyć też powiadomienia o logowaniach z innych urządzeń lub o nieudanych próbach logowania, jeśli taka opcja jest dostępna na platformie społecznościowej. Co jakiś czas sprawdzaj aplikacje mające dostęp do twojego konta i odinstaluj te, których nie używasz. Regularnie aktualizuj oprogramowanie zabezpieczające przeglądarkę i aplikacje. Łącz się tylko ze sprawdzonymi i bezpiecznymi sieciami. Unikaj zwłaszcza logowania się do konta podczas korzystania z publicznej sieci Wi-Fi.

Źródła:

[1] Opoczka P.,*Włamanie się na cudze konto w mediach społecznościowych*, Infor, 28 III 2022 r., https://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/5442947,Wlamanie-sie-na-cudze-konto-w-mediach-spolecznosciowych.html.

[2] *Kradzież tożsamości w internecie - jak się bronić?*, G Data, https://gdata.pl/przewodnik/kradziez-tozsamosci-w-internecie.

[3] *Co zrobić, gdy ktoś przejął Twoje konto na Facebooku?*, BGK, https://www.bgk.pl/bezpieczenstwo/cyberbezpieczenstwo/historie-prawdziwe/co-zrobic-gdy-ktos-przejal-twoje-konto-na-facebooku/.

fundacja instytut
CYBERBEZPIECZEŃSTWA

www.instytutcyber.pl