

Ćwiczenie – Rozpoznaj swoje ryzykowne internetowe przyzwyczajenia (Wersja dla nauczyciela)

Informacja dla nauczyciela: Tekst oznaczony kolorem czerwonym lub wyróżniony kolorem szarym jest dostępny wyłącznie w wersji dla nauczyciela.

Zadania

Pomyśl o działaniach w Internecie, które mogą zagrażać Twojemu bezpieczeństwu lub prywatności.

Wprowadzenie

Internet potrafi być groźnym miejscem, dlatego musisz być czujny w celu zapewnienia bezpieczeństwa swoich danych. Napastnicy są pomysłowi oraz gotowi posłużyć się przeróżnymi chwytami, aby tylko zmylić swoje ofiary. W tym ćwiczeniu dowiesz się, co jest ryzykownym działaniem w Internecie oraz zapoznasz się ze sposobami zwiększenia swojego bezpieczeństwa.

Część1 Zapoznaj się z warunkami świadczenia usług.

Odpowiedz szczerze na poniższe pytania i zapisuj punkty za każdą odpowiedź. Podsumuj wszystkie punkty i przejdź do części 2, aby dokonać analizy swoich zachowań w Internecie.

- a. Jakiego rodzaju informacje udostępniasz w serwisach społecznościowych? _____
 - 1) Wszystko; media społecznościowe są dla mnie podstawą kontaktu ze znajomymi i rodziną. (3 punkty)
 - 2) Wybrane przeze mnie artykuły i aktualności (2 punkty)
 - 3) To zależy; wybieram to, co chcę udostępnić i komu chcę udostępnić. (1 punkt)
 - 4) Nic; nie korzystam z mediów społecznościowych. (0 punktów)
- b. Kiedy zakładasz nowe konto w serwisie internetowym: _____
 - 1) Używam tego samego hasła w różnych serwisach, aby ułatwić sobie jego zapamiętanie. (3 punkty)
 - 2) Tworzę hasło, które jest tak proste, jak to tylko możliwe, abym mógł je łatwo zapamiętać. (3 punkty)
 - 3) Wymyślam bardzo złożone hasło i zapisuję je w menedżerze haseł. (1 punkt)
 - 4) Wymyślam hasło, które jest podobne do hasła używanego w innym serwisie, ale nie jest identyczne. (1 punkt)
 - 5) Wymyślam całkowicie nowe, silne hasło. (0 punktów)
- c. Po otrzymaniu wiadomości e-mail zawierającej odnośniki do innych witryn: _____
 - 1) Nie klikam odnośników, ponieważ wyznaję zasadę ignorowania e-mailowych linków. (0 punktów)
 - 2) Klikam w odnośnik, ponieważ e-mail został już przeskanowany przez serwer pod kątem zagrożeń. (3 punkty)
 - 3) Klikam we wszystkie odnośniki, jeśli wiadomość e-mail pochodzi od znanej mi osoby. (2 punkty)
 - 4) Wskazuję kursorem odnośniki, aby zweryfikować docelowy adres URL przed kliknięciem. (1 punkt)
- d. Podczas wizyty na stronie internetowej wyskakuje nowe okienko (ang. pop-up window). Informuje ono o istniejącym zagrożeniu dla Twojego komputera oraz proponuje pobranie i instalację programu diagnostycznego, który zabezpieczy Twój komputer: _____
 - 1) Klikam, pobieram i instaluję program, aby zabezpieczyć komputer. (3 punkty)

- 2) Sprawdzam wyskakujące okna, wskazuję kursorem na odnośnik, aby zweryfikować jego prawidłowość. (3 punkty)
- 3) Ignoruję komunikat, zamykam odwiedzaną stronę. (0 punktów)
- e. Kiedy potrzebujesz zalogować się na stronę swojego banku: _____
 - 1) Natychmiast wprowadzam swoje dane logowania. (3 punkty)
 - 2) Zanim zacznę wprowadzać jakiegokolwiek dane weryfikuję adres internetowy, aby upewnić się, że jestem na stronie swojego banku. (0 punktów)
 - 3) Nie korzystam z bankowości internetowej. (0 punktów)
- f. Przeczytałeś artykuł na temat pewnej aplikacji i decydujesz się ją wypróbować. Podczas przeszukiwania Internetu znajdujesz wersję próbną aplikacji na nieznanej witrynie: _____
 - 1) Szybko pobieram i instaluję aplikację. (3 punkty)
 - 2) Wyszukuję informacje na temat twórcy aplikacji przed jej pobraniem. (1 punkt)
 - 3) Nie pobieram ani nie instaluję aplikacji. (0 punktów)
- g. W drodze do pracy znajdujesz na ulicy nośnik USB. _____
 - 1) Zabieram go ze sobą i podłączam do komputera, aby obejrzeć zawartość. (3 punkty)
 - 2) Zabieram go ze sobą i podłączam do komputera, aby całkowicie usunąć jego zawartość przed ponownym użyciem. (3 punkty)
 - 3) Zabieram go ze sobą i podłączam do komputera. Uruchamiam skanowanie antywirusowe, aby móc go używać do swoich celów. (3 punkty)
 - 4) Nie podnoszę go. (0 punktów)
- h. Chcesz połączyć się z Internetem. Znajdujesz darmowy punkt dostępu Wi-Fi (hotspot). W takiej sytuacji: _____
 - 1) Łączę się z nim i korzystam z Internetu. (3 punkty)
 - 2) Nie łączę się z nim, zamiast tego szukam innego zaufanego połączenia. (0 punktów)
 - 3) Łączę się z nim i nawiązuję połączenie korzystając z bezpiecznej usługi VPN przed wysłaniem jakichkolwiek danych. (0 punktów)

Część2 Przeanalizuj swoje zachowania w Internecie

Im wyższy wynik, tym mniej bezpieczne są Twoje zachowania w Internecie. Celem jest stuprocentowe bezpieczeństwo. Można to osiągnąć poprzez zwracanie uwagi na wszystkie działania wykonywane w Internecie. Jest to bardzo ważne, ponieważ nawet jeden mały błąd może mieć daleko idące skutki.

Dodaj wszystkie punkty z części 1. Zapisz swój wynik. _____

0: Jesteś bardzo bezpieczny w Internecie.

0 – 3: Jesteś dość bezpieczny w Internecie, ale powinieneś pracować nad wyeliminowaniem ryzykownych zachowań.

3 – 17: Twoje zachowanie w Internecie jest dość niebezpieczne, istnieje wysokie ryzyko ataku.

18 lub więcej: Twoje zachowanie w Internecie jest bardzo niebezpieczne, potencjalny atak jest tylko kwestią czasu.

Poniżej znajduje się kilka ważnych wskazówek dotyczących bezpieczeństwa w Internecie.

- a. Im więcej informacji udostępniasz w mediach społecznościowych, tym bardziej pozwalasz osobie atakującej Ciebie poznać. Większa wiedza o Tobie pozwala atakującemu przeprowadzić o wiele bardziej ukierunkowany atak. Na przykład udostępniasz publicznie informacje o wyścigach samochodowych, które

oglądałeś na żywo. Napastnik może stworzyć złośliwego e-maila, w którym będzie podszywał się pod platformę biletową z interesującą Cię ofertą. Ponieważ właśnie uczestniczyłeś w takim wydarzeniu, e-mail będzie wydawał się bardziej wiarygodny.

- b. Wielokrotne wykorzystywanie tego samego hasła jest złym nawykiem. Jeśli użyjesz takiego hasła w serwisie, który jest pod kontrolą cyberprzestępców, to są oni zdolni użyć tego hasła do zalogowania się w Twoim imieniu w innych serwisach.
- c. Wiadomości e-mail można łatwo sfałszować w taki sposób, aby sprawiały wrażenie, że pochodzą z oficjalnego źródła. Sfałszowane wiadomości e-mail często zawierają odnośniki do złośliwych witryn lub złośliwego oprogramowania. Zgodnie z ogólną zasadą nie klikaj odnośników otrzymanych w wiadomościach e-mail.
- d. Nie pobieraj żadnego oprogramowania z niepewnych źródeł, szczególnie jeśli pochodzi ono z przypadkowej strony internetowej. Jest bardzo mało prawdopodobne, aby przypadkowa strona internetowa oferowała Ci ważną aktualizację oprogramowania. W takiej sytuacji zdecydowanie zalecane jest zamknięcie przeglądarki i użycie narzędzi dostępnych w systemie operacyjnym do sprawdzenia dostępności aktualizacji.
- e. Stworzenie złośliwej strony internetowej, która do złudzenia przypomina stronę banku, nie jest trudnym zadaniem. Dokładnie sprawdź adres internetowy zanim klikniesz w odnośniki lub podasz jakiegokolwiek ważne informacje. Upewnij się, że znajdujesz się na właściwej stronie internetowej.
- f. Kiedy pozwalasz programowi działać na Twoim komputerze, oddajesz mu część władzy nad systemem. Zastanów się dobrze zanim uruchomisz nieznany program. Przeszukaj Internet i upewnij się, że osoba lub firma będąca autorem programu jest godna zaufania. Programy pobieraj tylko z wiarygodnych źródeł: oficjalnych stron internetowych ich producentów lub autorów.
- g. Napędy i nośniki USB mają wbudowane małe kontrolery, które pozwalają im na komunikację z komputerem. Istnieje możliwość przeprogramowania tego kontrolera, tak aby nośnik USB powodował instalację złośliwego oprogramowania na podłączanych do niego komputerach. Złośliwe oprogramowanie zostaje ukryte w kontrolerze urządzenia USB, a nie w obszarze przechowującym dane. Wobec tego ani czyszczenie pamięci ani skanowanie antywirusowe nie spowoduje jego usunięcia.
- h. Atakujący często uruchamiają fałszywe darmowe punkty dostępowe Wi-Fi (hotspoty), aby przyciągnąć do nich użytkowników. Użytkownicy podłączeni do takiego punktu dostępowego są zagrożeni, ponieważ napastnik ma dostęp do wszystkich informacji przesyłanych za jego pośrednictwem. Nigdy nie używaj nieznanych darmowych punktów dostępowych Wi-Fi bez szyfrowanej transmisji danych za pośrednictwem VPN. Nigdy nie podawaj poufnych danych, takich jak numery kart kredytowych podczas korzystania z nieznanej sieci (przewodowej lub bezprzewodowej).

Do przemyślenia:

Wykonałeś analizę swojego zachowania w Internecie. Jakie zmiany wprowadzisz, by zwiększyć swoje bezpieczeństwo w sieci?

Odpowiedzi mogą być różne.