[FRONTCOVER]

[Start Community Language Document 1]

Bezpieczeństwo w cyberprzestrzeni

Ogólnokrajowe Centrum Bezpieczeństwa Cybernetycznego (*National Cyber Security Centre*) – wydanie w formatach odmiennych.

Niniejsze materiały zebrała organizacja charytatywna Lead Scotland przy współpracy z Oddziałem ds. Bezpieczeństwa Cybernetycznego (*Cyber Resilience Unit*) i dzięki funduszom rządu szkockiego.

Poradnik ten powstał w oparciu o informacje dostępne na stronie internetowej National Cyber Security Centre.

Informacje, przetłumaczone na języki Unii, zawarto w następujących 7 dokumentach:

- Niniejszy poradnik, który obejmuje wstęp i 6 zalecanych sposobów zabezpieczania się w cyberprzestrzeni.
- Odrębne szczegółowe dokumenty wyjaśniające każdy z 6 kroków, jakie należy podjąć.
- Wszystkie odnośne linki dostępne są na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego https://www.ncsc.gov.uk/cyberaware/.

6 sposobów zabezpieczenia się w cyberprzestrzeni

Z uwagi na pandemię koronawirusa, ludzie znacznie więcej czasu w tym roku spędzają w cyberprzestrzeni.

Daje to hakerom znacznie więcej możliwości na przeprowadzenie cyberataków.

Przedmiotem ich ataków są często ludzie i przedsiębiorstwa, a metody, jakie do tego stosują to:

- Oszustwa drogą mailową lub internetową.
- Oprogramowania złośliwe – są to programy, które potrafią uszkodzić urządzenia komputerowe lub ułatwić hakerom dostęp.

Jeśli hakerzy uzyskają dostęp do urządzenia lub konta, mogą zdobyć nasze pieniądze, dane osobowe lub informacje na temat naszej firmy.

Aby zabezpieczyć się w cyberprzestrzeni, należy zastosować następujące środki:

Środek 1 – Ustaw silne, niepowtarzalne hasło dla poczty elektronicznej.

Środek 2 - Stwórz silne hasła używając 3 przypadkowych słów.

Środek 3 – Zapisz swoje hasła w przeglądarce.

Środek 4 – Uruchom dwustopniową weryfikację (2FA).

Środek 5 – Uaktualnij oprogramowanie swoich urządzeń.

Środek 6 – Sporządź kopię zapasową swoich danych.

[End Community Language Document 1]

[Start Community Language Document 2]

ŚRODEK 1 – Ustaw silne, niepowtarzalne hasło dla poczty elektronicznej

Gdy haker zdobędzie dostęp do naszej poczty elektronicznej, będzie w stanie zmienić hasła dostępu do innych kont i zdobyć zapisane informacje dotyczące naszych danych osobowych lub naszej firmy.

Hasło dostępu do poczty elektronicznej powinno być mocne i nie należy go używać jako dostępu do innych kont. Dzięki temu hakerom będzie trudniej je złamać lub odgadnąć.

Użycie trzech przypadkowych słów to dobry sposób na stworzenie mocnego, niepowtarzalnego hasła, które łatwo zapamiętać. Omówimy to szczegółowo w dalszej części poradnika.

Należy również chronić inne ważne konta, takie jak konta bankowa czy konta portali społecznościowych.

Dlaczego adres poczty elektronicznej jest tak ważny?

Adres mailowy to jedno z najważniejszych kont. A dlaczego hakerom tak na tym zależy?

Wyobraź sobie, że haker uzyskuje dostęp do twojego maila.

Może dzięki temu zdobyć Twoje dane osobowe, które masz zapisane, albo skontaktować się z ludźmi, podszywając się pod Ciebie.

Najgorsze jednak jest to, że może Ci uniemożliwić dostęp do wszystkich Twoich kont w sieci. Może tego dokonać w ten sposób, że wejdzie na jakieś Twoje konto i użyje funkcji „Nie pamiętam hasła”. Mail z linkiem do zmiany hasła zostanie wysłany na Twojego maila, a haker użyje go, by uniemożliwić Ci dostęp do tego konta.

Gdy haker zmieni hasło dostępu do jednego konta, będzie mógł nadal zmieniać wszystkie Twoje hasła.

Jak więc można zabezpieczyć swój adres mailowy i utrudnić hakerom dostęp do swoich kont w sieci?

Należy stosować silne hasło dla poczty elektronicznej i nie powtarzać tego samego hasła na innych kontach. Dzięki temu, nawet jeśli ktoś złamie hasło dostępu do jednego konta, nie będzie mógł go użyć, aby uzyskać dostęp do Twojego maila.

Pamiętaj, że Twój adres mailowy to jedno z najważniejszych kont. Zabezpiecz je dobrze.

Jak zmienić hasło dostępu do poczty elektronicznej

Jak zmienić hasło w poczcie:

- Gmail
- Yahoo!
- Outlook
- BT
- AOL Mail

Jeśli rodzaj serwera, jakiego używasz nie jest podany powyżej, znajdź w sieci informacje na temat tego, jak uzyskać wskazówki od dostawcy na temat zmiany hasła.

Wskazówki dla przedsiębiorców indywidulanych i małych firm dotyczące haseł

Konta właścicieli firm mogą zawierać informacje poufne dotyczące klientów, firmy i środków finansowych.

Jeśli konta nie są odpowiednio zabezpieczone, zwiększa się ryzyko, że firma może paść ofiarą cyberataku. Ryzyko może być natury prawnej lub finansowej, ale może również dotyczyć naruszenia rozporządzenia o ochronie danych osobowych (RODO).

Jeśli firma zatrudnia pracowników, należy zadbać o to, by nie przechowywali haseł w pobliżu urządzeń i aby blokowali lub wyłączali urządzenia, których nie używają.

Dalsze informacje dostępne są na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego w poradniku dla małych firm – Small Business Guide.

Wszystkie odnośne linki dostępne są na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 2]

[Start Community Language Document 3]

ŚRODEK 2 Stwórz silne hasła używając 3 przypadkowych słów

Trudno zapamiętać wszystkie hasła ustawione na swoich ważnych kontach, gdy każde jest inne.

Dobrą metodą tworzenia silnych, łatwych do zapamiętania haseł jest użycie trzech przypadkowych słów.

Nie należy używać słów, które łatwo odgadnąć (na przykład imię zwierzątka domowego). W razie potrzeby można dodać cyfry i symbole. Na przykład: CzerwonePortkiDrzew4!

Zapisywanie haseł w wyszukiwarce pomoże nimi operować. Omówimy to szczegółowo w dalszej części poradnika.

Sprawdź swoją umiejętność tworzenia silnych haseł

Zgadnij, które z tych haseł nie znalazło się na liście 100,000 najczęściej rozszyfrowywanych haseł?

- arsenal22
- 1v&upjw3nt
- p@55w0rd
- CzerwonePortkiDrzew
- Victoria!
- 2011977

Odpowiedź: CzerwonePortkiDrzew.

Hakerzy wymieniają między sobą listy zawierające miliony rozszyfrowanych haseł.

3 przypadkowe słowa to łatwiejszy sposób tworzenia nowych haseł, które będą przypisane wyłącznie Tobie i dlatego trudniejsze do odgadnięcia.

Wszystkie odnośne linki dostępne są na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego https://www.ncsc.gov.uk/cyberaware/.

[End Community Language Document 3]

[Start Community Language Document 4]

ŚRODEK 3 Zapisz swoje hasła w przeglądarce

Zapisywanie haseł w przeglądarce polega na tym, że zezwalasz swojej przeglądarce (np. Chrome, Safari lub Edge) zapamiętać swoje hasło.

Dzięki temu:

- Hasło nam nie zginie i nie trzeba go zapamiętywać samemu.
- Jesteśmy chronieni przed pewnymi rodzajami przestępstw cybernetycznych, jak na przykład sfałszowane strony internetowe.

Jest to lepsze zabezpieczenie niż słabe hasła czy stosowanie tego samego hasła dla różnych kont.
Zapisane hasła należy jednak zabezpieczyć, na wypadek zguby lub kradzieży urządzenia.

Jak zabezpieczyć zapisane hasła

Gdyby ktoś zdobył dostęp do Twojego urządzenia, mógłby użyć zapisanych haseł, aby wejść na Twoje konta.

Do tego rodzaju przestępstw cybernetycznych dochodzi znacznie rzadziej niż ataki hakerów przez internet w celu rozszyfrowywania haseł za pomocą specjalnego oprogramowania.

Aby się zabezpieczyć, należy:

- Wyłączyć lub zablokować urządzenie, gdy się go nie używa.
- Stosować silne hasło dostępu do urządzenia.
- Uruchomić dwuetapową weryfikację we wszystkich urządzeniach i na wszystkich kontach.
- Udostępnić zabezpieczenie biometryczne (czytnik rysów twarzy lub linii papilarnych), jeśli jest ono dostępne w naszym urządzeniu.

Należy również regularnie wykonywać kopie zapasowe danych. Dzięki temu będzie można je łatwo odtworzyć w razie zgubienia lub kradzieży urządzenia.

Jak zapisywać swoje hasła w przeglądarce

Jak zapisywać hasła w następujących przeglądarkach:

- Google Chrome
- Microsoft Edge
- Firefox
- Safari

Czy wiesz?

Twoje hasła będą dostępne na wszystkich urządzeniach, jeśli się zalogujesz w tej samej przeglądarce.

Dodatkowe zabezpieczenie

Utworzywszy silne hasła, oddzielne dla każdego urządzenia i konta (środki od 1 do 3), należy następnie zastosować dodatkowe środki (od 4 do 6), aby ograniczyć ryzyko nielegalnego dostępu przez hakerów.

Wszystkie odnośne linki dostępne są na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document 4]

[Start Community Language Document 5]

ŚRODEK 4 Uruchom weryfikację dwustopniową (2FA)

Weryfikacja dwustopniowa (2FA) uniemożliwia hakerom dostęp do konta, nawet jeśli uda im się zdobyć hasło.

Niektóre banki internetowe automatycznie stosują weryfikację dwustopniową, wymagając dodatkowych informacji na potwierdzenie tożsamości, na przykład kodu, który przesyłany jest na telefon.

Jak uruchomić weryfikację dwustopniową (2FA)

Większość kont wymaga manualnego uruchomienia 2FA, choć nie wszystkie konta oferują taką weryfikację. Banki internetowe automatycznie stosują weryfikację dwustopniową.
Weryfikacja dwustopniowa 2FA nazywana jest inaczej uwierzytelnieniem wieloczynnikowym.

WIDEO: Jak działa weryfikacja 2FA

Wideo o tym, jak działa 2FA można obejrzeć na YouTube.

Jak uruchomić weryfikację 2FA dla poczty elektronicznej:

- Gmail
- Yahoo
- Outlook
- AOL

Jak uruchomić weryfikację 2FA dla kont w mediach społecznościowych:

- Instagram
- Facebook
- Twitter
- LinkedIn

Wszystkie odnośne linki dostępne są na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego https://www.ncsc.gov.uk/cyberaware/.

[End Community Language Document 5]

[Start Community Language Document 6]

ŚRODEK 5: Uaktualnij oprogramowanie swoich urządzeń

Nieuaktualnione oprogramowania, aplikacje i systemy operacyjne są osłabione, przez co łatwiej się do nich włamać.

Producenci starają się zapobiegać tym słabym punktom wydając aktualizacje. Aktualizowanie urządzenia i oprogramowania pozwala chronić się przed hakerami.

Należy uruchomić automatyczne aktualizowanie urządzeń i programów, które mają tę funkcję. Nie trzeba wtedy pamiętać o tym, by regularnie je aktualizować.

Niektóre urządzenia i programy wymagają aktualizacji manualnej. W telefonie lub komputerze pojawiają się wtedy przypomnienia. Nie należy ich ignorować. Aktualizacja programów zapewnia bezpieczeństwo w internecie.

Jak uruchomić automatyczne aktualizowanie

Jak uruchomić automatyczne aktualizowanie następujących urządzeń i programów:

- Apple - Mac
- Apple - iPhone and iPad
- Microsoft Windows 10. – wyszukaj aktualizację dla Windows 10
- System Windows 7 nie jest już obsługiwany. Należy go zaktualizować do Windows 10
- Smartfony i tablety typu Android
- Aplikacje Android

Pytanie: W jaki sposób producenci naprawiają słabe punkty swoich programów?

- bandaż
- łata
- naprawa

Odpowiedź: Gdy producent odkryje słaby punkt w swoim oprogramowaniu, wprowadza tzw. ‘łatkę’, aby to naprawić. W ten sposób dane są zabezpieczone.

Wszystkie odnośne linki dostępne są na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego https://www.ncsc.gov.uk/cyberaware/.

[End Community Language Document 6]

[Start Community Language Document 7]

ŚRODEK 6 - Sporządź kopię zapasową swoich danych

Tworzenie zapasowych kopii polega na skopiowaniu swoich danych na inne urządzenie lub w pamięci w chmurze.

Regularne kopiowanie sprawia, że zawsze mamy zapisane aktualne informacje. Dzięki temu szybciej można odtworzyć dane w razie kradzieży lub zniszczenia.

Dostępne jest również automatyczne tworzenie kopii zapasowych. W ten sposób informacje są regularnie zapisywane w pamięci w chmurze i nie trzeba o tym pamiętać.

Jeśli kopia zapasowa zapisana jest na nośniku USB lub na dysku zewnętrznym, należy go odłączyć od komputera, gdy tworzenie kopii zapasowej zostanie zakończone.

Czy wiesz?

Przed aktualizacją urządzenia, należy zawsze sporządzić kopię zapasową, ponieważ niektóre uaktualnienia mogą zmieniać lub usuwać pliki.

Jak uruchomić automatyczne sporządzanie kopii zapasowej

Jak uruchomić automatyczne zapisywanie kopii zapasowej dla następujących urządzeń i programów:

- Apple – Mac
- Apple - iPhone i iPad
- Android
- Microsoft Windows 10 i Windows 8 OneDrive

Wskazówki dla małych firm i indywidualnych przedsiębiorców na temat zapisywania kopii zapasowej

Sporządzanie kopii zapasowej danych pozwoli firmie działać w razie, gdyby padła ofiarą cyberataku.
Najpierw należy ustalić, jakie dane są dla firmy najważniejsze – dane dot. finansów, kontrakty, listy klientów lub dostawców. Kapie zapasowe trzeba sporządzać regularnie. Trzeba również wiedzieć, jak odzyskać dane z kopii zapasowej w razie utraty danych. Dalsze informacje można znaleźć w poradniku dla małych firm dostępnym na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego.
Wszystkie odnośne linki dostępne są na stronie internetowej Ogólnokrajowego Centrum Bezpieczeństwa Cybernetycznego https://www.ncsc.gov.uk/cyberaware/

[End Community Language Document7]

[END OF DOCUMENT]