

DOBRE NAWYKI DAJĄ WYNIKI

Kto w sieci uważa, ten się nie naraża



MADRA GŁOWA TO PRZECHOWA

Komentarze, polubienia, opublikowane zdjęcia to nasze cyfrowe ślady, które zostawiamy po sobie w internecie. Pojedynczo mogą nie mieć dużego znaczenia, ale kiedy się je połączy, umożliwiają tzw. profilowanie i mogą być źródłem wiedzy o użytkownikach. Internetowi przestępcy gromadzą tego typu informacje w celu zawstydzenia, zastraszenia lub wywołania u ofiary poczucia zagrożenia. Takie działanie nazywane jest doxingiem (z ang. docs, czyli dokumenty oraz compiling/releasing przetwarzać/upubliczniać).

Zadbaj o swoją prywatność w internecie. Zwracaj uwagę na oglądane i udostępniane przez siebie informacje, a przede wszystkim pamiętaj, że każda – nawet z pozoru nieistotna informacja, może być cenna dla cyberprzestępców.

QUIZ

1. Uzupełnij luki, wpisując słowa z ramki. W ten sposób poznasz ważne zasady cyberbezpieczeństwa.

- Nie otwieraj maili ani załączników
- Twórz i zmieniaj je regularnie.
- Nie klikaj w linki z niepewnych źródeł, nie wchodź na strony WWW, które są podejrzane, oraz pamiętaj o strony WWW.
- Zabezpiecz urządzenia elektroniczne, np. telefon, laptop, hasłem, kodem PIN lub (np. odcisk palca).
- Zwracaj uwagę na, czyli wzbudzające zainteresowanie chwytliwe tytuły lub miniaturki, które mają nakłonić do jakiegoś działania, np. zakupu towaru lub usługi.

clickbaity	sprawdzeniu certyfikatu	nieznanego pochodzenia	silne hasła	danymi biometrycznymi
------------	-------------------------	------------------------	-------------	-----------------------

2. Cyfrowe ślady to:

- informacje, które pozostawiamy po sobie, korzystając z internetu, np. opublikowane komentarze, zdjęcia, polubienia, oglądane lub udostępniane pliki,
- dokumenty w wersji cyfrowej, np. e-dowód,
- pliki, które mamy na swoich urządzeniach, np. filmy, muzyka, zdjęcia.

3. Połącz pojęcie z opisem.

Złośliwe oprogramowanie

Aplikacja, która dla bezpieczeństwa dzieci daje możliwość sprawdzania ich aktywności w sieci oraz blokowania dostępu do stron zawierających nieodpowiednie dla nich materiały. Pozwala też ustawiać limity czasowe, w których dzieci mogą korzystać z urządzeń ekranowych.

Spoofing telefoniczny

Podszywanie się pod dany nr telefonu – także z naszej książki adresowej. Na wyświetlaczu widzimy nazwę kontaktu zapisanego na swoim urządzeniu lub nazwę instytucji, która rzekomo do nas dzwoni (np. banku), a w rzeczywistości dzwoni do nas cyberoszust.

Aplikacja do kontroli rodzicielskiej

Szkodliwe programy, które uniemożliwiają lub zakłócają prawidłowe korzystanie z urządzeń elektronicznych, np. komputera, smartfona czy tabletu. Mogą ukryć dane, zmieniać je, a nawet przechwycić funkcje urządzenia czy szpiegować działanie użytkownika.

Klucz odpowiedzi:

1. nieznanego pochodzenia / silne hasła / sprawdzeniu certyfikatu / danymi biometrycznymi / clickbaity

2. A.

3.

3. Szkodliwe oprogramowanie – szkodliwe programy, które uniemożliwiają lub zakłócają prawidłowe korzystanie z urządzeń elektronicznych, np. komputera, smartfona czy tabletu. Mogą ukryć dane, zmieniać je, a nawet przechwycić funkcje urządzenia czy szpiegować działanie użytkownika.
2. Spoofing telefoniczny – podszywanie się pod dany nr telefonu – także z naszej książki adresowej. Na wyświetlaczu widzimy nazwę kontaktu zapisanego na swoim urządzeniu lub nazwę instytucji, która rzekomo do nas dzwoni (np. banku), a w rzeczywistości dzwoni do nas cyberoszust.
1. Aplikacja do kontroli rodzicielskiej – aplikacja, która dla bezpieczeństwa dzieci daje możliwość sprawdzania ich aktywności w sieci oraz blokowania dostępu do stron zawierających nieodpowiednie dla nich materiały. Pozwala też ustawiać limity czasowe, w których dzieci mogą korzystać z urządzeń ekranowych.