ZAMKNIJ SWÓJ INTERNET

Zamykasz swój dom, samochód i cenne rzeczy, ale... czy zamykasz swój Internet?

Join us on Facebook
Facebook/derbycc
Facebook/SaferDerbyCity

Follow us on Twitter
@DerbyCC
@SaferDerbyCity

Derby City Council

Internet jest wspaniały – od zakupów po kontakty towarzyskie, świat stoi dla Ciebie otworem. Zastanów się, czy dałbyś komuś swoją kartę bankową z numerem PIN, czy zostawiłbyś otwarte drzwi frontowe lub czy dałbyś swój komputer obcej osobie?

'Lock up Online' i powstrzymaj Złodzieja Internetowego przed dostaniem się do Twojego świata. Przeczytaj nasze wskazówki, które uchronią Cię przed zostaniem ofiarą zbrodni Internetowych.

'Zamknij się' w drodze

Nie pozwól, aby Twój telefon lub tablet wpadły w ręce Złodziei Internetowych.

- Nie zostawiaj ich na wierzchu w otwartej torebce, na siedzeniach lub widocznych w samochodzie
- Zabezpiecz swój telefon za pomocą długopisu UV i zarejestruj go na stronie takiej jak **www.immobilise.com**
- Użyj hasła lub PINu, aby zablokować urządzenie
- Zapisz numery seryjne IMEI, które znajdują się na baterii lub karcie SIM. Można je uzyskać wybierając *#06#
- Ogranicz używanie alternatywnej sieci. Sieci Wi-Fi niezabezpieczone hasłem są nie tylko niebezpieczne, ale też wykańczają baterię
- Unikaj załączania Bluetooth, ochroń je hasłem
- Upewnij się, że wiesz jakie dane zapisują się w Twoim telefonie podczas synchronizacji z komputerem
- Synchronizuj reguralnie swój telefon.

ZAMKNIJ SWÓJ INTERNET

CYBERaCRIME
www.derby.gov.uk/lockuponline

Ślusarz

Więcej informacji i porad można znaleźć na: www.derby.gov.uk/lockuponline lub:

Zgłoś oszustwo: **www.actionfraud.org.uk**
Dowiedz się więcej: **www.getsafeonline.org.uk**
Bezpieczna bankowość: **www.banksafeonline.org.uk**
Zgłoś nielegalne treści: **www.iwf.org.uk**

Dowiedz się więcej na temat bezpieczeństwa dzieci w Internecie: www.childnet-int.org lub www.ceop.police.uk

Przygotowany na oszustwo

Złodzieje Internetowi uwielbiają zarabiać na oszustwach, bądź o jeden krok przed nimi i nie daj się oszukać.

Rodzaje oszustw i ważne wskazówki:

Fałszywe strony internetowe
- Bądź świadomy/a podczas kupowania biletów i wakacji przez Internet
- Korzystaj z renomowanych stron
- Sprawdzaj recenzje.

Fałszywe emaile
- Jeśli nie jesteś pewny/a emaila nie otwieraj go, nie klikaj w żadne linki ani załączniki
- Nigdy nie odpowiadaj na maile proszące o pieniądze lub dane personalne, nawet jeśli wydaje się, że to email od przyjaciela
- Nie odpowiadaj na groźby.

Strony aukcyjne
- Dokładnie przeczytaj szczegóły na temat produktu
- Sprawdź recenzje i zadawaj pytania
- Zostaw opinię (informację zwrotną)
- Dowiedz się więcej, strony aukcyjne oferują informacje na temat bezpieczeństwa
- Nie spiesz się z licytacją ani zakupem produktów
- Nie licytuj na więcej niż zamierzałeś/aś
- Nie zgaduj ani niczego z góry nie zakładaj.

Reklamy
- Zdaj sobie sprawę z 'mądrego namierzania', jeśli właśnie ogłosiłeś/aś na Facebooku, że się zaręczyłeś/aś, nagle zacznie pojawiać się więcej reklam dotyczących ślubów
- Nie zapisuj się na coś, czego nie chcesz
- Nie nabieraj się na obietnice darmowych produktów lub fałszywych nagród.

Wzbogać się szybko
- To prawie zawsze powoduje, że stajesz się biedniejszy, a nie bogatszy, wystrzegaj się.

Zamknij i zrób kopię zapasową

Zamykasz swój dom, samochód i cenne rzeczy, a co z Internetem? Zablokuj Złodziei Internetowych w komputerze i swoim życiu.

Wskazówki na temat haseł
- Nie używaj wszędzie tego samego hasła
- Jeśli zmieniasz hasło, użyj całkiem innego niż poprzednie
- Nie trzymaj swojego hasła obok komputera ani nie zapisuj go na nim
- Nie klikaj w 'zapamiętaj hasło dla tej strony'
- Unikaj używania dat urodzin/rocznic/imion zwierząt/nazw drużyn piłkarskich itp.
- Używaj dużych i małych liter, liczb i symboli.

Wskazówki
- Używaj antywirusa i upewnij się, że jesteś chroniony
- Zawsze instaluj aktualizacje
- Upewnij się, że Twój komputer ma hasło, kiedy go załączasz
- Nie sprawdzaj swoich prywatnych informacji, kiedy używasz darmowej i niechronionej sieci Wi-Fi
- Zawsze zabezpieczaj swoją sieć Wi-Fi silnym hasłem
- Zrób kopie zapasowe używając płytek CD, twardych dysków lub urządzeń USB
- Zakoduj swoje urządzenie USB
- Sprawdź zapory firewall. Większość jest darmowa i dostępna do ściągnięcia przez Internet
- Nie przetrzymuj prywatnych informacji w dokumentach lub ręcznych notatkach obok komputera.

Zamknij swoje życie

Złodziej Internetowy ma wiele twarzy, nie oddawaj swojej tożsamości, nie zapraszaj niechcianych 'przyjaciół' do swoich portali społecznościowych, chroń swoje życie!

Portale społecznościowe
Facebook, YouTube oraz Twitter są częścią codziennego życia. Uważaj co publikujesz, może to zostać użyte do popełnienia przestępstwa przeciwko Tobie.
- Jeśli nieznajomy na ulicy poprosiłby Cię o informację, czy udzieliłbyś jej? Jeśli odpowiedź brzmi nie, nie umieszczaj tego w Internecie
- Dowiedz się więcej o ustawieniach prywatności i dziel się tylko tym, co uważasz za stosowne
- Zgłaszaj naruszenia prywatności
- Rozmawiaj ze swoimi dziećmi o ryzykach jakie niosą ze sobą portale społecznościowe, na przykład pokoje do chatu, gry internetowe i klikanie w niewłaściwe rzeczy
- Bądź świadomy ukrytych kosztów gier i aplikacji, aby nie dostać dużego rachunku
- Dowiedz się więcej o ochronie haseł i kontroli rodzicielskiej.

Zakupy Internetowe
- Czy ta strona jest respektowana?
- Czy podczas płatności pojawia się ikonka bezpieczeństwa, zwykle kłódka, w prawym dolnym rogu lub na pasku adresu?
- Czy oferta wydaje się zbyt atrakcyjna?
- Czy strona wydaje się nietypowa?

Zgłoś to do www.actionfraud.org.uk Centrum Zgłaszania Oszustw w UK

Bankowość przez Internet
- Przyjrzyj się stronie dokładnie, jeśli coś wydaje się nie w porządku, to prawdopodobnie tak jest
- Nie zapisuj haseł do bankowości Internetowej i nie zostawiaj ich w pobliżu komputera
- Bądź czujny, gdy dostajesz emaile domniemanie z Twojego banku,nie klikaj w linki i nie podawaj detali swojego konta
- Czasem bank może pomóc, jeśli pojawi się problem działaj szybko.