Netoobrona

Gdy gówno trafi na wiatrak — a trafi — zacznie się wyłączanie Internetu. Wtedy będzie już *za późno*, by sie przygotować. Więc przygotujmy się dzisiaj!

Weź ten plik ze sobą, wydrukowany lub na urządzeniu. Podziel się z innymi.

Dostęp do Sieci

Te narzędzia pomogą w przypadku blokowania dostępu do konkretnych stron (np. zablokownaia społecznościówek, portali medialnych, strony Strajku Kobiet, itp), oraz niektórych sposobów blokowania dostępu do Internetu w ogóle.

1. **Tor**
   Absolutna podstawa to pobranie przeglądarki Tor. Pobierz ją *teraz*, nie odkładaj na później. Zablokowanie sieci Tor jest wyjątkowo trudne, ale musisz wpierw mieć do niej dostęp.
2. **VPNy**
   Jeśli masz dostęp do VPNów, jest to niezła metoda obchodzenia cenzury Sieci. Jeśli nie masz, nie przejmuj się, Tor w zupełności wystarczy.

Sieciowa obrona konieczna

Władze lub różne grupy z nią sprzymierzone będą próbowały włamywać się na nasze konta, podsłuchiwać naszą komunikację, zbierać o nas dane "na później". Na szczęście mamy jak się bronić.

Twoje urządzenia

Być może nie wszystkie poniższe porady da się zastosować na Twoim urządzeniu. Trudno. Zastosuj te, które się da.

1. **na bieżąco instaluj aktualizacje bezpieczeństwa, *zwłaszcza* jeśli wybierasz się na protest**
   luki bezpieczeństwa wykorzystywane są regularnie do włamań na urządzenia w celu śledzenia użytkowniczek/ów
2. **włącz blokadę ekranu i szyfrowanie pamięci**
   szyfrowanie jest włączone domyślnie na w miarę nowych urządzeniach z jabłuszkiem, na Androidach bywa różnie
3. **wyłącz biometryczne metody odblokowywania ekranu (odciski palców, skan oka czy twarzy, itp)**
   w przypadku biometrii wystarczająco fizycznie silny przeciwnik może po prostu siłą przyłożyć Twój palec do czytnika czy umieścić Twoją twarz przed kamerą

4. **przejdź na apkową dietę: odinstaluj nieużywane aplikacje, instaluj tylko apki których naprawdę potrzebujesz, uważaj z zezwoleniami**
   po co latarce dostęp do kontaktów i Internetu? czy ta gra na pewno jest tylko grą? każda apka może być niebezpieczna; zachowaj rewolucyjną czujność!
5. **przełącz urządzenie w tryb "wyłącznie LTE" (jeśli Twoje urządzenie to wspiera)**
   możesz to zrobić w ustawieniach sieci; starsze typy sieci mobilnych (2G/3G/3.5G) miały poważne luki ułatwiające przechwytywanie informacji w locie

Komunikacja

Dekadę temu w Rosji informacja, że ktoś jest gejem była nieistotna; dziś informacja, że dekadę temu ktoś był gejem może zrujnować tam komuś życie. Sieć nie zapomina; nie wiemy, co z rzeczy, o których dziś rozmawiamy swobodnie, za tydzień, miesiąc, czy rok będzie niebezpieczne.

Jeśli rozmawiasz o rzeczach potencjalnie wrażliwych, używaj bezpiecznych narzędzi. Godne polecenia:

1. **Signal**
   https://signal.org/
   Bezapelacyjnie najbardziej godny polecenia z punktu widzenia bezpieczeństwa komunikacji. Używany przez dziennikarki/rzy śledcze/ych, sprawdzony w boju, z rzeszą użytkowniczek/ków. Jeśli tylko możesz przerzucić się na Signala, zrób to.
2. **WhatsApp**
   Kontrolowany przez Facebooka, ale z szyfrowaniem zaimplementowanym przez ludzi z Signala. Jeśli możesz, wybierz Signala. Jeśli nie, WhatsApp też dobry.
3. **Briar**
   https://briarproject.org/
   Podstawowa zaleta: można sie komunikować przez Bluetooth i WiFi bez dostępu do Internetu. Nie mniej (a może i bardziej!) bezpieczny niż Signal.
   Podstawowe wady: mniej przyjazny w użyciu, mało użytkowniczek/ów, brak aplikacji na urządzenia z jabłuszkiem (tylko Android).

UWAGA! Wszelkie inne komunikatory prawie na pewno są nieszyfrowane i niebezpieczne. Mowa tu *zwłaszcza* o Messengerze, Telegramie, Viberze, Discordzie, czy Skypie. Tych rozwiązań należy unikać, zwłaszcza gdy rozmawiamy na tematy wrażliwe.
