imprezy niespodzianki.
– To prawda. Ani szyfrowanie dysku, ani szyfrowanie maili nie wpływa zauważalnie na codzienną obsługę komputera. Wszystko dzieje się automatycznie, nie zmieniając komfortu pracy. A zaszyfrowany dysk chroni nas przecież przed nieprzyjemnościami np. w wypadku pospolitej kradzieży. Pamiętaj też, że na niezaszyfrowany dysk łatwo można wgrać kompromitujące materiały. Tym sposobem ktoś, kto nie zrobił nic złego nagle może stać się przestępcą. Szyfrowanie dysku to kwestia zdrowego rozsądku. Zaś jeśli idzie o wiadomości to sam fakt, że szyfrujesz komunikację jest łatwy do wykrycia. Więc lepiej robić to ciągle, a nie tylko wówczas gdy planuje się coś nietypowego. No i najlepiej szyfrować komunikację do wszystkich, a nie tylko do wybranych osób.
– Musimy więc szerzyć zwyczaj szyfrowania wśród naszych znajomych?
– Im więcej osób to robi, tym bezpieczniejsze jest to dla na wszystkich.

Po więcej informacji zajrzyj na strony (w języku angielskim):

ssd.eff.org

securityinabox.org

Tekst:

sudoriot.net

Rysunki:

Krzywa Kreska

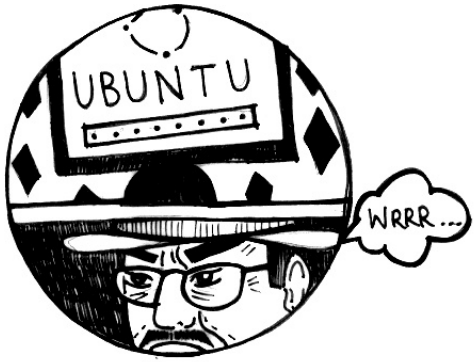
Julia i Zuza znały się od dawna, ale od pewnego czasu nie miały okazji się spotkać. Obowiązki dnia codziennego, zmiany pracy, przeprowadzki i problemy finansowe skutecznie to uniemożliwiały. Gdy jednak udało im się umówić, szybko znów odnalazły wspólny język. Omówiwszy swoje plany i nadzieje, zaczęły wspominać stare czasy. Doszły do wniosku, że wspaniale byłoby zorganizować spotkanie wszystkich dawnych znajomych, najlepiej w związku z jakąś okazją, tak aby pomysł nie wydał się zaproszonym gościom sztuczny.

Zaczęły przeglądać kalendarze w poszukiwaniu dobrego pretekstu, gdy nagle Zuza zauważyła zaznaczone dawno temu urodziny Natalii.
– Co ty na to – zwróciła się do Julii z wymownym uśmiechem, – aby zorganizować urodziny Natalii?
– To dobry pomysł – odpowiedziała koleżanka – Ostatnio nie była w najlepszym nastroju. Wspominała coś o tym, że brakuje jej kontaktu z ludźmi.
Po chwili namysłu Julia dodała jednak:
– Ale ciężko tak zorganizować urodziny komuś dorosłemu. Jubilaci zwykle sami się tym zajmują.
– Impreza niespodzianka?
– Ha, to jest pomysł!

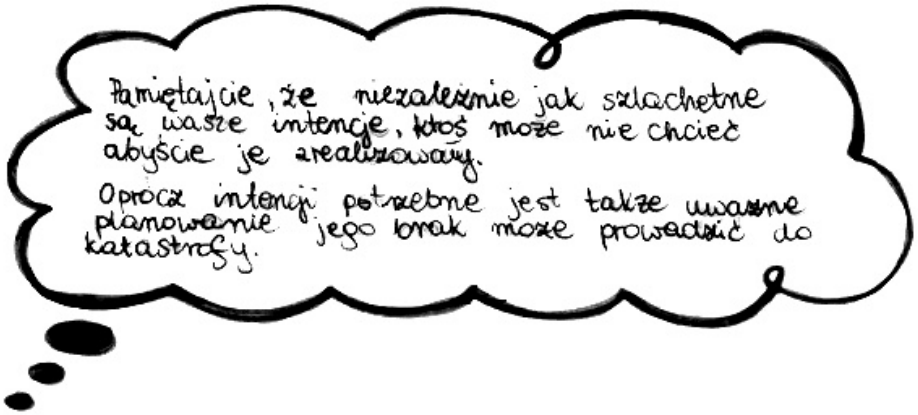
Koleżanki z entuzjazmem oddały się układaniu listy gości, omawianiu atrakcji i najważniejszego, czyli planu wyciągnięcia jubilatki na imprezę. Nagle Julia posmutniała.
– Pamiętasz Michała? – spytała. Michał, nienawistny osobnik, wytrwale pałający żądzą zepsucia każdej imprezy, uprzykrzał życie dziewczynom już za dawnych czasów. Utrzymywany przez rodziców, swój wolny czas wypełniał pieniędzy, czasu i determinacji, ale jest możliwe. Można także zmusić kogoś szantażem lub groźbą do wyjawienia hasła.
– Michał chyba nie posunie się aż tak daleko?
– My chcemy tylko zrobić imprezę niespodziankę. Ale gdybyśmy chciały np. zrobić coś nielegalnego, pozostałoby nam chyba zrezygnować z komunikacji zdalnej w ogóle. Ale na szczęście nic takiego nie planujemy.
– Imprezy niespodzianki wciąż są legalne – zaśmiała się Zuza.
– Tak, wypijmy za to.

Zuza i Julia pośmiały się chwile, nalały wina do kieliszków, po czym wróciły do głównego tematu rozmowy.
– Prawdopodobnie dla naszego projektu imprezy niespodzianki wystarczy, abyśmy używały maili zabezpieczonych PGP, do których klucze znajdują się na zaszyfrowanych dyskach. Komputer z Ubuntu pozwala załatwić to w naprawdę prosty sposób – ucieszyła się Zuza.
– Tak, o ile nie wygadamy wszystkiego niepowołanym osobom przy pierwszej okazji! – tym razem tylko Julia się roześmiała. – Musimy pamiętać, że żadne narzędzie nie zagwarantuje powodzenia projtu. Mamy ustaloną listę kluczowych informacji. Wiemy, że ostatecznie i tak je wszystkie ujawnimy, bo impreza przecież po prostu się odbędzie. Ale musimy przemyśleć dokładnie kiedy i komu ujawniamy każdą z nich.

– Słusznie – przyznała Zuza. – Właściwie, pomyślałam sobie, że to wszystko o czym rozmawiamy jest tak łatwe, że powinnyśmy stosować to zawsze, nie tylko wtedy gdy organizujemy



z pendrive'a i w czasie instalacji zaznaczyć odpowiednie kwadraciki kliknięciem myszki. To załatwia sprawę. Ubuntu jest darmowy i łatwy w obsłudze, możemy więc łatwo namówić tych z naszych gości, którzy wciąż używają Windowsa, na zmianę systemu operacyjnego.
– Użycie Ubuntu, lub innego łatwego w obsłudze Linuxa i zaszyfrowanie dysku w czasie instalacji systemu to niezły pomysł – znów zgodziła się Julia. – To takie zabezpieczenie jak dobre drzwi antywłamaniowe z podwójnym zamkiem. Oczywiście nic nie dają jak zostawi się je otwarte, albo jak złodzieje wejdą oknem. Jeśli korzystasz z zaszyfrowanego dysku, aby chronić swój klucz prywatny musisz pamiętać, że jeśli komputer jest włączony, to dysk jest odszyfrowany. A to oznacza, że nigdy nie możesz zostawiać włączonego komputera bez opieki (nawet, gdy ekran jest zablokowany) oraz, że nie możesz nikomu podawać swojego hasła odszyfrowującego komputer! Ale nawet jeśli dochowasz tych zasad istnieją pewne sposoby by wykraść klucz. Ale fakt, że są one na tyle trudne, że być może Michał nie będzie chciał się w nie bawić.
– Wiem. Można przecież włamać się przez sieć do pracującego komputera, wtedy dysk jest niezaszyfrowany – Zuza nie dała się zaskoczyć. – Ale przed takimi atakami chroni regularne aktualizowanie całego oprogramowania komputera (co w Ubuntu akurat jest bardzo proste) i unikanie ryzykownych zachowań, np. otwierania plików z niezaufanych źródeł.
– Masz rację. Przy zachowaniu podstawowych zasad komputer z zaszyfrowanym dyskiem i Ubuntu to twardy orzech do zgryzienia. Przynajmniej jeśli hasło odblokowujące ma kilkanaście znaków. Ale potencjalnemu atakującemu zostają jeszcze najbardziej brutalne metody. Są np. urządzenia, które zainstalowane w pokoju zapisują hasła wpisywane z klawiatury komputera. Aby je zainstalować trzeba się włamać do mieszkania, więc wymaga to

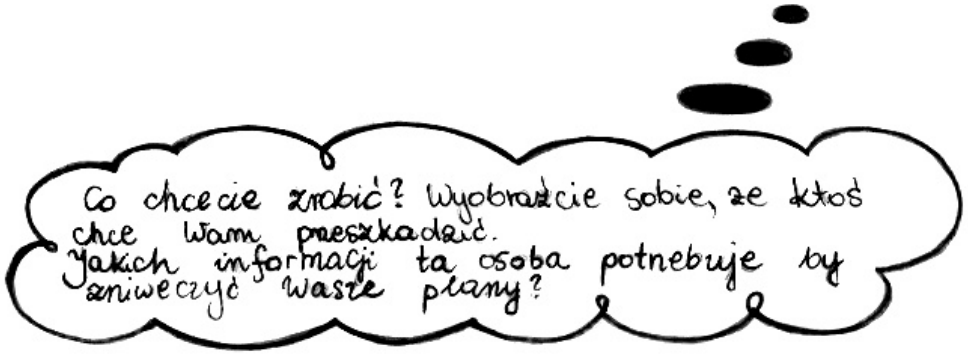


wcinaniem kebabów, siedzeniem na wykopie i kombinowaniem jak pokrzyżować plany chcącym się nieco rozerwać koleżankom.

– Tak – odparła Zuza ściągając brwi z namysłu. – Jestem przekonana, że kiedy tylko się dowie, to zrobi wszystko żeby zepsuć zabawę. Poinformuje Natalię, albo w ogóle wmanipuluje ją w jakiś wyjazd za miasto akurat w ten dzień. Albo przekaże gościom fałszywe informacje co do czasu i miejsca. Ale czy sądzisz, że to możliwe aby wpadł na trop naszej imprezy?
– Nie możemy tego wykluczyć. Michał ma liczne znajomości, pieniądze i jest bardzo wpływowy – zauważyła ze smutkiem Julia.
– Poza tym nie zajmuje się prawie niczym innym.
– Dawno nic nie robiłyśmy. Może trochę o nas zapomniał. Tak czy inaczej myślę, że musimy spróbować. Jeśli zrobimy to rozsądnie, Michał nie znajdzie na nas sposobu.

1. Analiza zagrożeń

Pierwszym problemem omówionym przez dziewczyny to lista informacji, które nie mogą za żadne skarby wejść w posiadanie Michała.
– Nie ma sensu, abyśmy robiły wielką tajemnicę z byle czego – zauważyła Zuza.



– Może i tak. Ale ktoś mi kiedyś powiedział, że jak o czymś wiedzą więcej niż dwie osoby to już nie jest sekret. Być może jest w tym pewna przesada, ale musimy ustalić listę szczególnie chronionych informacji. Dobrze by było, żeby tak długo jak będzie to możliwe, nie ujawniać ich nikomu – Julia zrobiła nieustępliwą minę.
– Dobrze. Chcemy zrobić imprezę niespodziankę. Skoro sam fakt, że ją przygotowujemy nie może być przedwcześnie wyjawiony Natalii, musimy chronić tę informację także przed innymi. Szczególnie przed Michałem.
– To że robimy taką imprezę, a także jej czas, miejsce oraz zaproszeni goście to będą nasze informacje krytyczne. Ujawnienie każdej z nich niewłaściwym osobom może utrudnić nam wykonanie zadania – Julia ucieszyła się w duchu, że tak szybko przeszły pierwszy etap. – Oczywiście część z nich ujawnimy naszym gościom, ale będziemy to robić stopniowo i z opóźnieniem, aby w razie ewentualnego przecieku Michał miał mało czasu na reakcję.
– Ale czy Michał to jedyna osoba, która może chcieć zepsuć tę imprezę? – spytała Julia.
Dziewczyny zastanawiały się przez chwilę. Tym razem nikt inny nie przyszedł im do głowy. Przez moment rozmawiały o tym, że gdyby chciały zorganizować imprezę w opuszczonej leśniczówce, w której kiedyś się spotykały, problemem mógłby być również okoliczny gajowy. Na razie wykluczyły jednak tę opcję i postanowiły się skupić na Michale.

– Enigmail rozwiązuje wiele problemów, to prawda. Musimy jednak zadbać o dodatkowe środki bezpieczeństwa. PGP działa w ten sposób, że każdy użytkownik ma parę kluczy: publiczny i prywatny. Swój klucz publiczny udostępniasz innym by mogli zaszyfrować wiadomość do ciebie.
Jest on, jak sama nazwa wskazuje, jawny i niezbędny do tego by napisać do ciebie zaszyfrowanego maila. Musisz więc wysłać swój klucz do mnie, ale możesz także umieścić go np. na swojej stronie www, czy na Facebooku. Sprawy mają się odwrotnie z kluczem prywatnym. Twoim kluczem prywatnym można odszyfrować każdą wiadomość adresowaną do ciebie. Jeśli ktoś zdobędzie twój, albo mój klucz prywatny, to nici z całej zabawy – zauważyła Julia. – Oba te klucze to zwykłe pliki, zapisane na dysku komputera. Jeśli więc napiszesz do mnie zaszyfrowanego maila, a ja nie zadbam o to, aby mój klucz prywatny był dobrze zabezpieczony, to narażę nas na kłopoty. Michał będzie mógł zdobyć mój klucz i odczytać nasze maile, a także podszyć się pode mnie i wprowadzić cię w błąd.
– Rozwiązaniem jest oczywiście zaszyfrowanie dysku komputera – powiedziała spokojnie Zuza. – Wówczas nawet jeśli Michał ukradnie mój komputer, a wiemy że już robił takie rzeczy, nie będzie w stanie odczytać zapisanych danych.

Koleżanki dotarły już do przytulnego mieszkania Zuzy i rozsiadły się wygodnie. Julia ucieszyła się, że mogą spokojnie napić się w znajomym wnętrzu i wreszcie poczuła się swobodnie. Popijając wino spokojnie kontynuowały rozmowę.

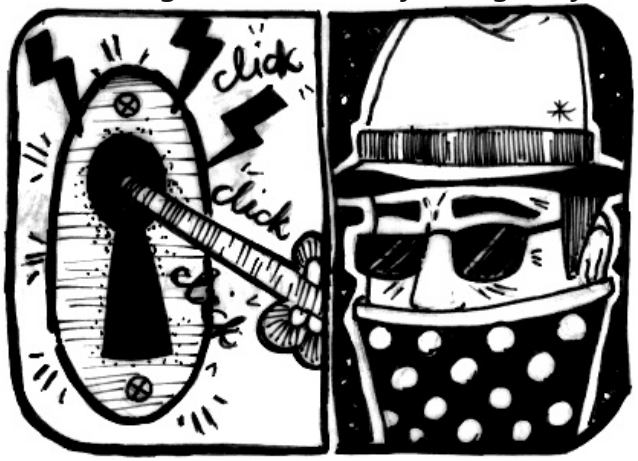
4. Szyfrowanie dysku

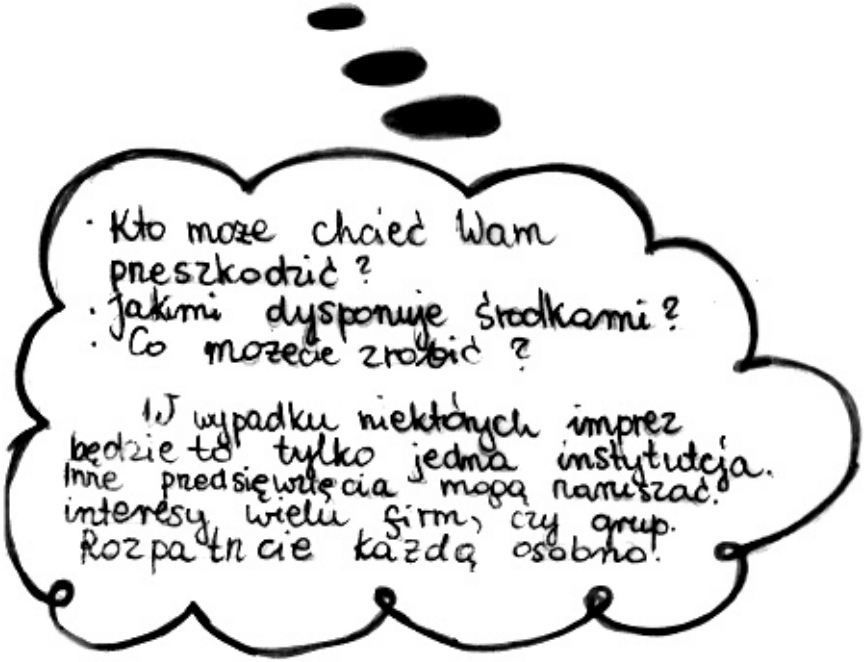
– Masz rację! Zaszyfrowanie całego systemu operacyjnego, lub po prostu danych użytkownika na dysku, znacząco utrudni Michałowi dostęp do naszych kluczy prywatnych. Nawet jeśli wejdzie do mojego mieszkania i włączy mój komputer to bez hasła zbyt wiele się nie dowie – przyznała Julia.
– Szczęśliwie to proste! Pamiętam, że Ubuntu proponuje to jako jedną z opcji dostępnych w czasie instalacji tego systemu operacyjnego. Jak ktoś nie używa jeszcze Ubuntu, lub nie ma zaszyfrowanego dysku, może uruchomić instalator Ubuntu

podejrzewamy, przekazują Michałowi dane swoich użytkowników. Nawet jak łączysz się przez HTTPS zaszyfrowana jest tylko komunikacja między twoim komputerem a serwerem. Dane na serwerze są widoczne dla każdego kto ma do niego dostęp, jak pocztówki leżące na poczcie –
– To prawda. Pamiętam jak jeden z naszych ulubionych operatorów poczty email okazał się kolegą Michała. A my się zastanawiałyśmy, dlaczego wszystkie działania rozsypują się w pył zanim wejdą w fazę końcowej realizacji! Michał i jego koledzy mieli nasze ustalenia na tacy! – przyznała Zuza. – To faktycznie oznacza, że potrzebujemy programu, który szyfruje wiadomości na moim komputerze, tak by odszyfrowane były dopiero przez ciebie. Wówczas przechwycenie ich pomiędzy naszymi maszynami nic nie da.

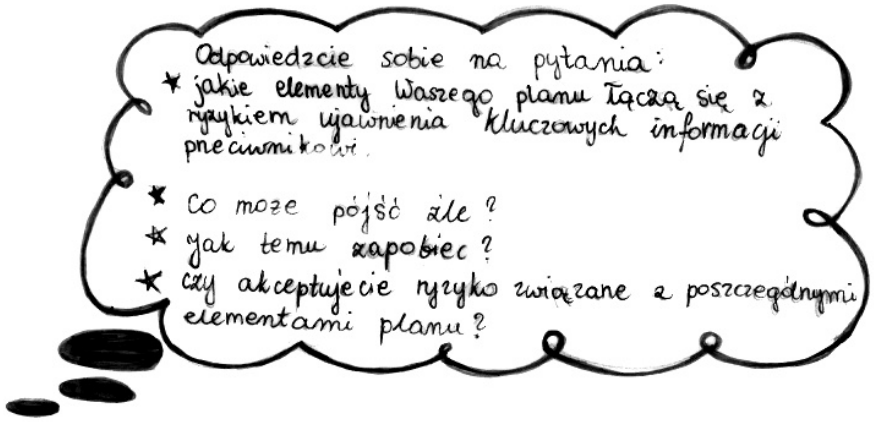
3. Szyfrowanie maili

– Tak się składa, że jest program, który daje taką możliwość. Nazywa się „Całkiem Niezła Prywatność", czyli „Pretty Good Privacy". Skrót to PGP, spotkać też można zapis PGP/GPG – Julia niezbyt ładnie się uśmiechnęła. – Chociaż ja bym go nazwała „Odrobina wolności".
– Tak, wiem o tym! – ucieszyła się Zuza. – Kiedyś byłam na szkoleniu z obsługi PGP, robionym przez lokalnych aktywistów. Pamiętam, że to było łatwe. Instalowało się program pocztowy Thunderbird i w nim dodatek Enigmail. Po krótkiej konfiguracji można było wysyłać maile zaszyfrowane PGP/GPG. Myślę, że nawet dziecko sobie z tym poradzi. Możemy to także zasugerować naszym gościom. Tak, by jak przekażemy im w ostatniej chwili miejsce zbiórki, ta informacja także była zaszyfrowana!



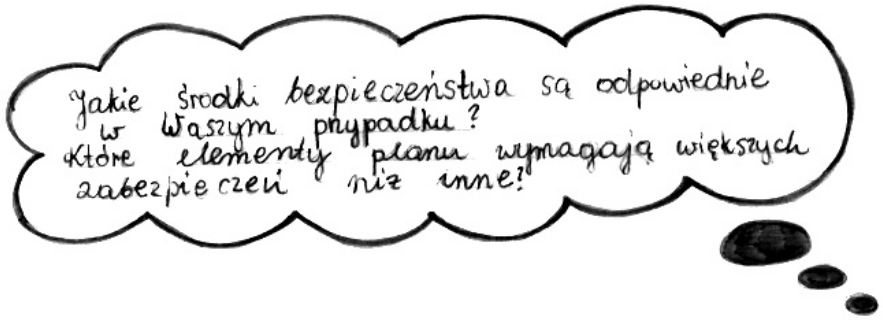


Wyniki dyskusji były jednak raczej przygnębiające. Michał miał znacznie więcej pieniędzy, czasu i sojuszników niż nasze bohaterki. Mógł rutynowo używać różnych środków by dowiedzieć się, czy dziewczyny nic nie planują, wszak pamiętał je jeszcze z dawnych czasów. Nie były też do końca pewne, czy niektórzy ich znajomi nie kolegują się z Michałem. To sprawiało, że cała operacja mogła być trudniejsza niż na początku zakładały.



2. HTTPS zamiast HTTP

– Raczej nie omówimy tego wszystkiego dzisiaj. Ustalenie szczegółów imprezy wymaga dużo czasu – zauważyła Julia.
– Trudno coś zrobić nie komunikując się zdalnie. Musimy rozmawiać przez Internet lub telefon – odparła Zuza. – Wiem, że myślisz już o związanych z tym ryzykach. Ale sądzę, że znajdziemy dobre sposoby. Nie będziemy mogły dotrzeć do wszystkich gości osobiście. Nie uda nam się też spotkać za każdym razem, gdy wydarzy się coś nieprzewidzianego. Mamy za mało czasu. Potrzebujemy bezpiecznego sposobu zdalnej komunikacji.
Julia strapiła się nieco.
– Najlepiej byłoby omawiać wszystko bezpośrednio. Moim zdaniem, jeśli zdalna komunikacja nie jest konieczna, zawsze w takich sytuacjach warto jej unikać. Na pewno Michał, tak jak przed laty, całymi dniami grzebie w nie swoich sprawach, przeczesuje Internet, podsłuchuje rozmowy telefoniczne, itp. – powiedziała. – Pamiętasz co nam opowiadał Kuba? Michał płacił mu za zakładanie sond, czyli komputerów instalowanych w studzienkach komunikacyjnych, które przechwytywały i zapisywały cały ruch od danego użytkownika nim przekazały go dalej. Nie możesz być pewna, że ja, ty, albo któryś z gości nie ma takiej sondy. A o telefonach to już zupełnie nie ma co rozmawiać.



– Tak. To prawda. Ale jeśli używasz HTTPS Michał nic nie odczyta z takiej sondy – zauważyła trzeźwo Zuza. – Prawie każdy popularny serwis, czy to mailowy, czy społecznościowy, domyślnie używa HTTPS. Jak łączysz się z Gmailem lub Facebookiem, Michał o tym wie, ale nie jest w stanie odczytać treści komunikacji.
– Używanie protokołu HTTPS zamiast HTTP to podstawa i wszystkie powinniśmy to robić. Ta dodatkowa literka „S” w adresie strony widoczna w pasku przeglądarki zapewnia, że nasza komunikacja nie może być łatwo podsłuchana. Faktem jest, że już większość stron internetowych, do których się logujemy, wymusza na nas używanie HTTPS. Utrudnia to przechwycenie naszych danych np. przez hakerów podsłuchujących Wi-Fi. Dobrym pomysłem jest zainstalowanie wtyczki do przeglądarki „HTTPS everywhere”, która rozpozna czy dana strona obsługuje HTTPS i włączy go nawet gdy jest to nieobowiązkowe. I jeśli nie jest to konieczne, najlepiej nie logować się do witryn, które nie obsługują takiego szyfrowania.
Zuza zamyśliła się na chwilę, rzuciła okiem na zegarek i zaproponowała:
– Wiesz co, dokończmy rozmowę u mnie w domu. Mam świetne wino, przy okazji trochę się pośmiejemy oglądając stare zdjęcia.
– Świetnie, dawno u ciebie nie byłam.

Koleżanki szybko się zebrały i kontynuowały rozmowę idąc ulicą. Julia podjęła przerwany wątek.

– Wracając do HTTPS, pomyślałam, że słaba to pociecha zwłaszcza gdy mówimy o Michale. Nie pamiętasz ilu on ma znajomych? Pracownicy wielu serwisów, w tym takich, których w ogóle o to nie