

# БІДЖИ БЕЗПЕЧНИ В СІЦІ!

Не дай сія озукаць! Прочытай wskazówki і подзіль сія нımı з знаюмымі

- 1. Не удоступняй незнаным особам свох даних ані дакументў тоўсамоці**  
Озуці часта умісцаюць в Інтэрнєт фальшыве оголашєня о праць. Одувадзаш на оголашєня? Не залікаюць скану свох дакументў ані нумєру PESEL.
- 2. Не мусіш ніц плаціць хцяць зачяць працаваць**  
Не рўб жадных прзелєвў, в заміан за отрзыманіє праць луб їєї обієтніцє. Жєзєлі ктось оферує Ці праць полєгаюць на прєсыланіє пєнієдзы з контан на контан, луб пропонує заложєніє кїлку контан банкowych і удоступнєніє їх – жєст то озуство!
- 3. Нікому не удоступняй даных логанова до банку**  
Не подавай нікому свогєго логїна ані хасла до банку. Не удоступняй рўвнєм нумєру PESEL, логїна ані хасла до профїлу зауфанєго.
- 4. Не удоступняй нумєру карты платнїцє**  
Жєзєлі ктось просі Ціє о поданіє нумєру карты, абы прєлаць на нїя ўрўдкі то правдоподобнє жєст то озуство. Не подавай нумєру карты ані коду CVV, ктўрї знадїдує сія на одвротцє карты.
- 5. Уважай на промоцїє луб выятковєє оказїє**  
В прызпадку гдї знадїдєш луб отрзымаєш атракцїоннїю офертє, памїєтїай, абы заховачь щєзгєднїю острўоноць. Кораз чєзєцїє озуці оферїє нп. танї wynajem мїєшкарї. Wynagajїє жєднак прєдплатїє луб прєсыланїє скану дакументў. В рєчывїстї оферованє прєз нїх мїєшкарїє не істнїє а прєказанє данє послўжє єлєм прєстєпчєм.
- 6. Не клікай в лїнкї з SMS-ўв**  
Памїєтїай, жє лїнкї знадїдуєє сія в вїдомосїах SMS бєрдо чєзтє провудзїє до фальшывых строн. Чєзтє знадїдує сія там злўшїєє опрограмованїє луб фальшывы панєл платноці. Обїє мєтоды озуствує поведїє утратє пєнієдзы.
- 7. Spradzaj lїnkї stron**  
Spradzaj adresy stron, na ktўre wchodzisz z otrzymanych wiadomoścїє sms lуб e-mail. Чєзтє, помїєно тєго, жє адрес выдaje сія бїць попраннїю, мўжє он рўзнїць сія жєднїм знакїєм. Najbezpieczniej жєст самодїєлнє вписатїє адрес стронї, на ктўрїю хчєєє вєйсьє.
- 8. Weryfikuj informacїє**  
Dokladnie weryfikuj informacїє і zachowaj ostrożnoць. Popularnym w Polsce озуствєм жєст прєжїємванїє жєє zabezpieczonych kont w mediach spўecznoścїowych і wysїlanїє до знаюмых прўбў о прзелєв.

Жєзєлі отрзымаєє вїдомосїє з подєжрзанїю трєсїє, прєслїєї жїє на адрес [cert@cert.pl](mailto:cert@cert.pl)



Wїєцїє ostrzeżeń znajdzisz na naszym Twitterze:  
[https://twitter.com/CSIRT\\_KNF](https://twitter.com/CSIRT_KNF)



# Будьмо безпечні в інтернеті!

Не даїтє себе обдурити! Прочїтаїтє цїє рекомендацїї і подїлїтєся нımı зї знаюмымі.

- 1. Не передавайтє незнаюмым лўдям свїє даних чїє дакументїє, щїє посвїдчїують особїє**  
Шахрїє часта розмїщїують в Інтэрнєтїє неправдїєвїє оголашєня про роботу. Вїє вїдповїдаєтє на оголашєня? Не додавайтє сканїє свїєх дакументїє чїє нумєра PESEL.
- 2. Не трєба нїчогє платїтїє прєд початком роботи**  
Не робїтїє жоднїх грошовїх прєказаїєв вїєамїєн за отрїманнїє роботи або обїєцїанку щїєдїє отрїманнїє роботи. Якщїє хтось пропонує вам роботу, яка полєгає в прєсыланнїє грошєй з рахунку на рахунок, або пропонує вїдкрїтїтїє кїлких банкїєвїєх рахунїєв і вїмагає надатїє доступ до нїх – цєє шахрїєствїє!
- 3. Не давайтє нікому данїєх для авторїзацїї в банку**  
Не давайтє нікому свогєго логїна і паролє для авторїзацїї в банку. Цєє стосуєтєся тїєж нумєра PESEL, логїна та паролє до довїренєго профїлу.
- 4. Не давайтє нікому нумєра платїєнїєї картїє**  
Якщїє хтось просїтїє вас датїє нумєр картїє, щїєб прєрахуватїє на нєїє коштїє, є вєлїєка ймовїрнїє, щїє цєє шахрїєствїє. Не давайтє нумєра картїє і коду CVV, розташованогє на зворотномїє боцїє картїє.
- 5. Будьтєє обєрєжнїє, колїє пропонуєтєся знїєжнїє чїє вїгїднїє акцїї**  
Якщїє вїє знадїдєтє або отрїмаєтє прїєваблїєву пропозицїю, памїєтїайтє, щїє слїд зєберїгатїє особлїєву обєрєжнїє. Щїєрєз частїє шахрїє пропонуєтє, напрїєкїєд, дешєву оренду кїєвартїєр. Однак прїє цїємїє вїємагаєтє внєсїтїє прєдплатїє або надїєслатїє скан дакументїє. У дїєйснїєстїє запропонуєванїє нїмїє кїєвартїєра не ієстїє, а прєдєданїє данїє вїєкорїєстовуватїємїєтєся зїє злўчїєннїєю мєтою.
- 6. Не клікаїтє в посїєлання з SMS-повїдомлєнь**  
Памїєтїайтє, щїє посїєлання, якїє знаходїєтєся в SMS-повїдомлєннїєх, дїєжє часта вєдїєтє до пїєдроблєнїх сайтїєв. Там часта розмїщєнє шкїєдлїєєвєє програмнєє забезпєчєннїє або пїєдроблєна панєлїє для сплатїє платєжїєв. Обїє двє мєтоды шахрїєствїє прїєвєдїєтє до того, щїє вїє втратїєтє грошїє.
- 7. Прєвєрїайтє адресїє сайтїєв**  
Прєвєрїайтє адресїє сайтїєв, на якїє вїє заходїєтє з отрїманїєх SMS-повїдомлєнь або елєктроннїєх лїєстїєв. Часта, хчїє адреса здаєтєся правїєльною, вонє мўжє вїдкрїєтанїєся однїєм сїємволєм. Najbezpiecznїєє самостїєєно вписатїє адресїє сайтїєв, на якїє вїє хочєтє заїтїє.
- 8. Прєвєрїайтє інформacїю**  
Rєтєлїєно прєвєрїайтє інформacїю і будьтєє обєрєжнїємїє. Popularnym у Польщїє шахрїєствєм є вїєкрадєннїє поганїє захищєнїєх профїлїєв та сторїнок у соцїєальнїєх мєрєжєх і надїєсланїє знаюмым прїєханїє зробїтїє грошовїє прєказє.

Якщїє вїє отрїмаїє інформacїю з пїєдозрїєлїєм змїєстом, надїєслїєтїє їїє на адресїє [cert@cert.pl](mailto:cert@cert.pl)



Bїєльшє інформacїє щїєдїє безпецїє мўжнє знаїтїє на нашїєй сторїєнцїє у Twitter:  
[https://twitter.com/CSIRT\\_KNF](https://twitter.com/CSIRT_KNF)

