

Informačná bezpečnosť a ochrana osobných údajov

Ing. Ivana Budinská, PhD.

budinska@savba.sk



#CyberSecMonth
#ThinkB4Uclick
cybersecuritymonth.eu



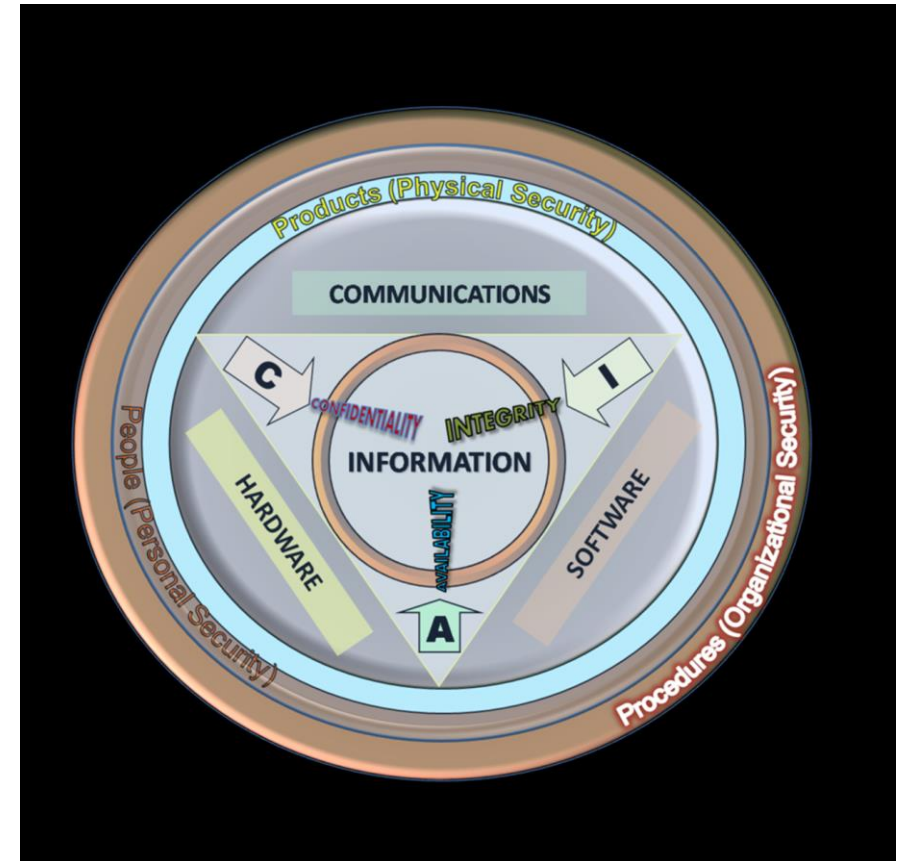
Čo je informačná bezpečnosť?

- Stav
 - dobre informovaný pocit istoty, že bezpečnostné riziká a bezpečnostné opatrenia sú v rovnováhe
- Proces
 - ako dosiahnuť daný stav
- Veda
 - multidisciplinárna, intergovaná
 - Počítačové vedy, sieťové technológie, kryptografia, sociológia, psychológia, kriminalistika, právo



Čoho sa týka IB?

- Všetkých komponentov informačných systémov
 - HW, SW, siete, prídavné zariadenia
 - Procedúry – fyzická bezpečnosť, organizačná bezpečnosť, ľudia
 - informácie
- CIA model IB – dôvernosť integrita dostupnosť



Čo na nás číha na internete

- Kybernetická kriminalita
 - nelegálna a trestná činnosť páchaná na komponentoch informačných systémov alebo pomocou informačných systémov (napr. bankové krádeže)
 - Porušovanie autorských práv, vydieranie, šírenie poplašných správ
 - Postihnuteľné aj našim trestným zákonom
- Kybernetické útoky
 - Často politicky motivované, snaha ovplyvniť politickú situáciu v krajine
 - Zahŕňa aj nelegálne zbieranie informácií
- Kybernetický terorizmus
 - Zneužitie informačných systémov na šírenie paniky, strachu
 - Priame ohrozenie životov, útoky vedené na kritickú infraštruktúru, vládne systémy, vojenské systémy



Aké metódy používajú útočníci?

- Malvér
 - Vírusy, červy, trójske kone, spyware, adware, ransomware, botnet
- Phishing
 - Metódy sociálneho inžinierstva
- Spoofing
 - Ukradnutie identity
- DDoS
 - Odmietnutie služby, zahltenie servera množstvom falošných požiadaviek
- M-i-t-M
 - Odpočúvanie, alebo iná forma ukradnutia dát počas komunikácie



Autentifikácia

- Znalosť – niečo, čo vieme (pin kód, heslo)
- Vlastníctvo – niečo, čo máme (token, hw zariadenie, mobil, banková karta)
- Vlastná existencia – niečo, čo sme (biometrické spôsoby autentifikácie)
- Multifaktorová autentifikácia



Login a heslo

- PC, tablet, smartphone, internetové služby – e-mail, sociálne siete, e-banking
- Najčastejšie útoky
 - slovníkový útok – zoznamy najčastejšie používaných hesiel
 - Útok hrubou silou – vyžaduje veľký výpočtový výkon, napr. cloud, kvantové počítače znamenajú prelom v rýchlosti a výkone
 - Aktívne útoky – infiltrácia zariadenia škodlivým kódom, phishing, vishing, MitM

Rank	2011 ^[6]	2012 ^[7]	2013 ^[8]	2014 ^[9]	2015 ^[10]	2016 ^[5]	2017 ^[11]	2018 ^[12]	2019 ^[13]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty	111111
10	dragon	baseball	adobe123 ^[a]	football	baseball	1234	iloveyou	iloveyou	123123

Najpoužívanéjšie heslá							
1.	123456	6.	123456789	11.	123123	16.	1234
2.	password	7.	111111	12.	admin	17.	monkey
3.	12345678	8.	1234567	13.	1234567890	18.	shadow
4.	qwerty	9.	iloveyou	14.	letmein	19.	sunshine
5.	abc123	10.	adobe123	15.	photoshop	20.	12345

Ochrana – používanie silných hesiel

- Dĺžka hesla je dôležitejšia, ako je zložitosť – aspoň 12 znakov
- Nepoužívať univerzálne heslá
- Nepoužívať triviálne heslá
- Neprezradiť heslo
- Používať antivir a aktualizovať systém
- Prihlasovať sa iba z dôveryhodných zariadení
- Vyhybať sa verejným sieťam

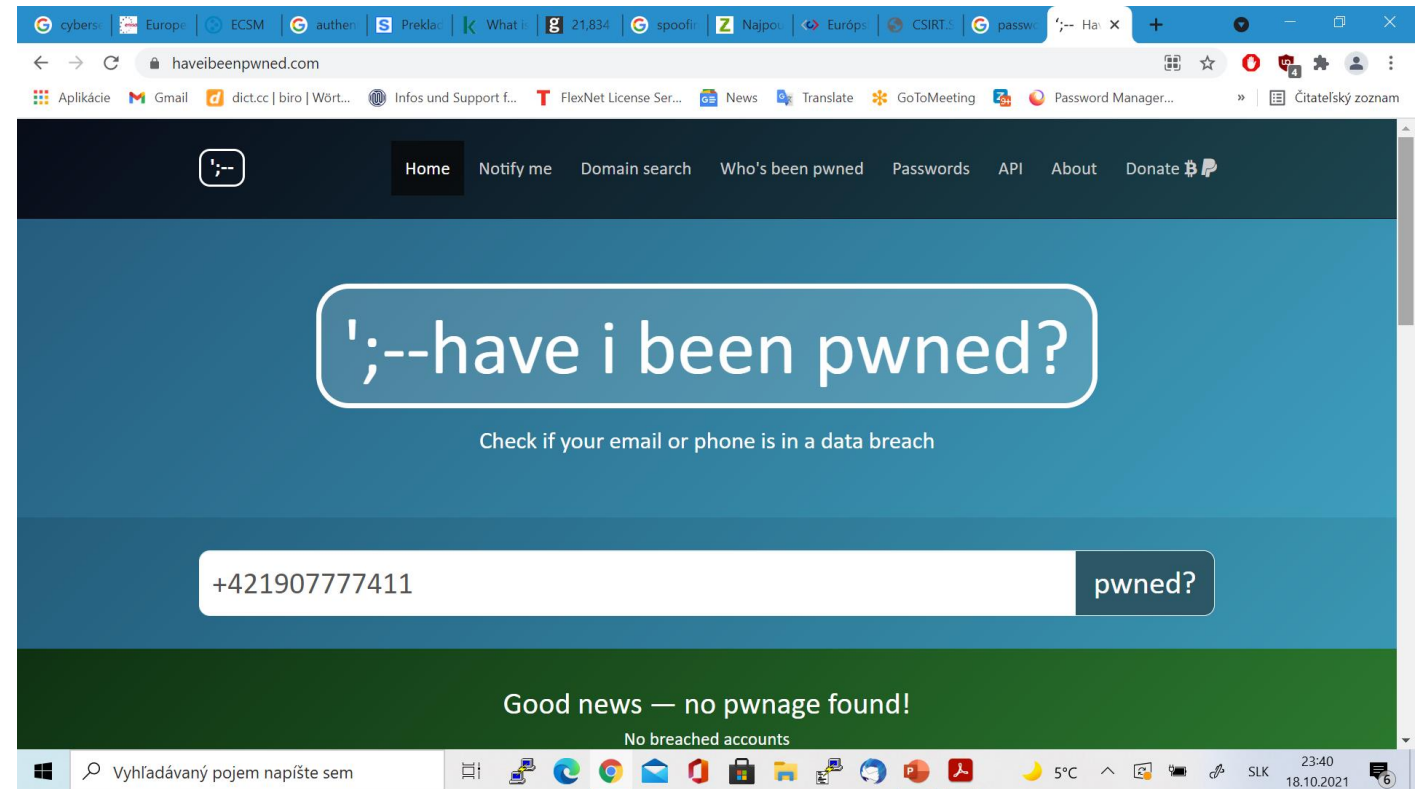


Ako zistím, či heslo bolo kompromitované?

- Služba
<https://haveibeenpwned.com/>
- Používanie bezpečné systéme na ukladanie hesiel
- Prehliadače, google

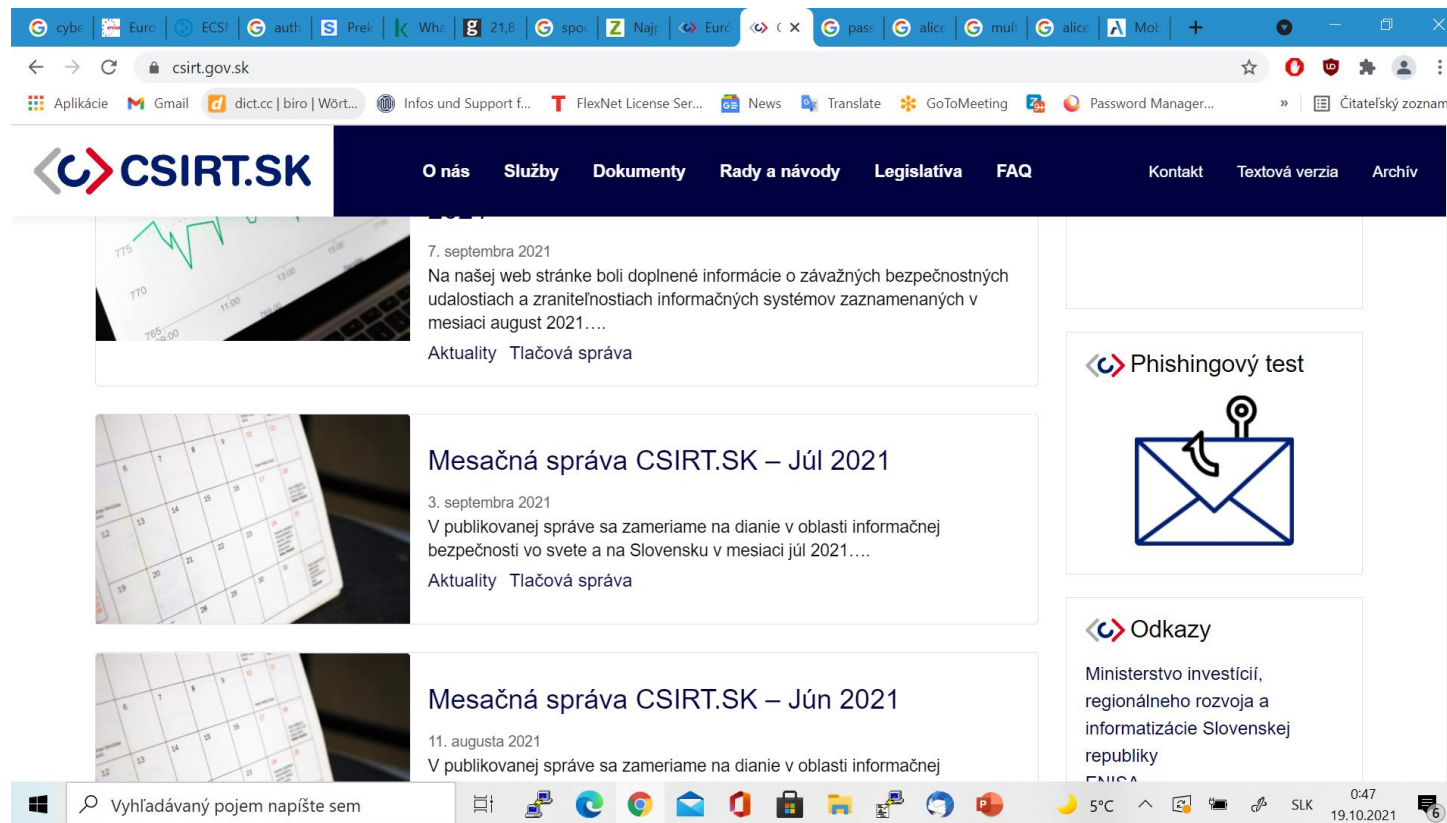
Ochrana hesla na strane servera

- Hashovanie, solenie, monitorovanie neúspešných prihlásení



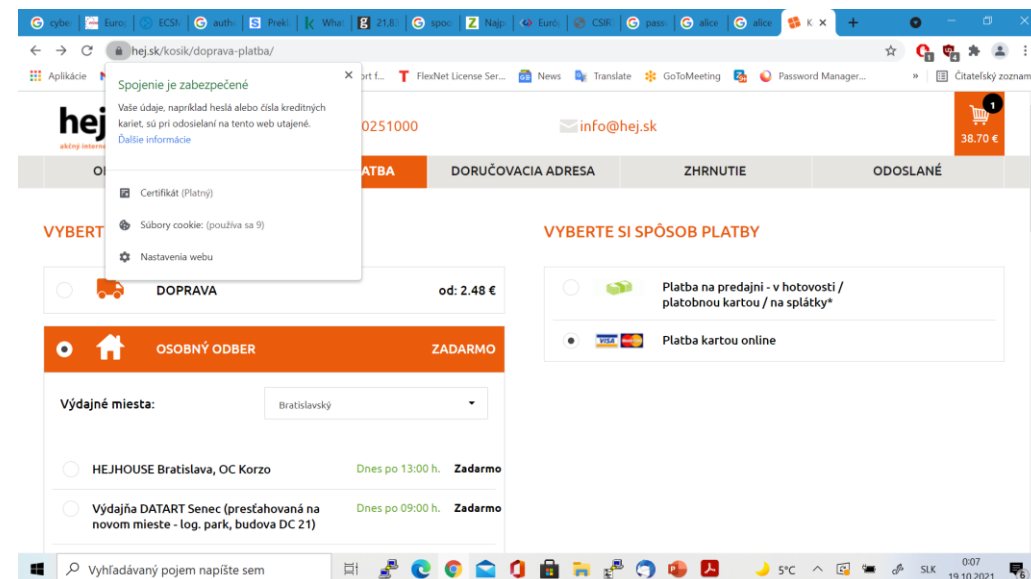
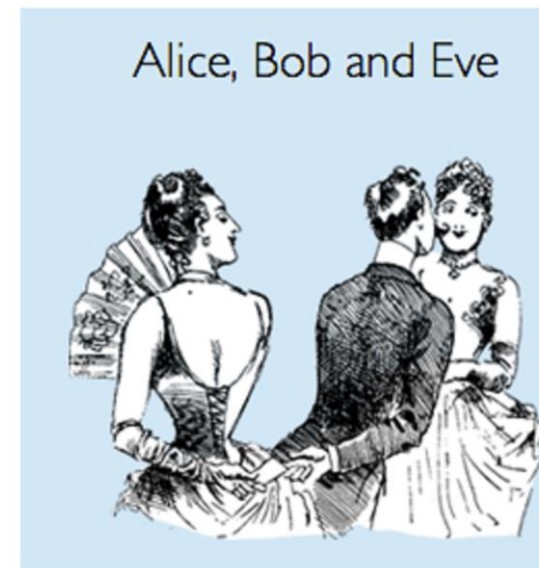
Phishingový test

- CSIRT – Computer Security Incident Response Team
- <https://www.csirt.gov.sk/archiv/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html?csrt=16313759056537423783>



Alice and Bob – najznámejší pár v kryptografii

- Útoky počas komunikácie – odpočúvanie (Eve - eavesdropper), MitM
- Ochrana spočíva v kryptografii – šifrovanie správ
- Vo verejných sieťach preferujeme spojenie cez VPN
- Vždy kontrolovať zabezpečenie pripojenia po celú dobu a certifikáty





Upcoming updates to file-based Domain Control Validation

In compliance with upcoming policy changes set out by the CA Browser (CA/B) Forum, changes to file-based Domain Control Validation are being made by Sectigo on November 15, 2021.

Learn more at sectigo.com/DCVChange

[Home](#) > CPS Repository

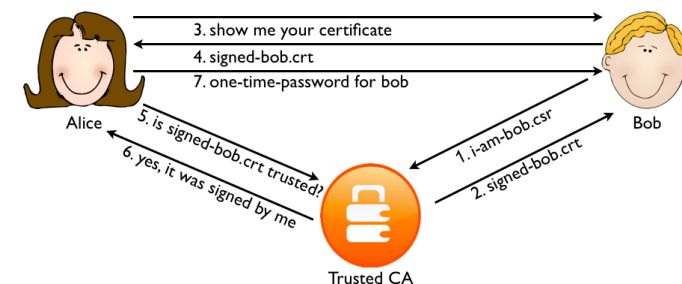
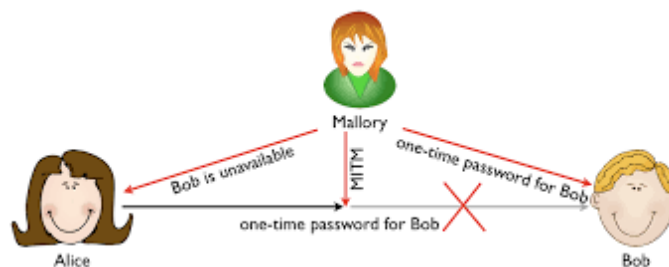
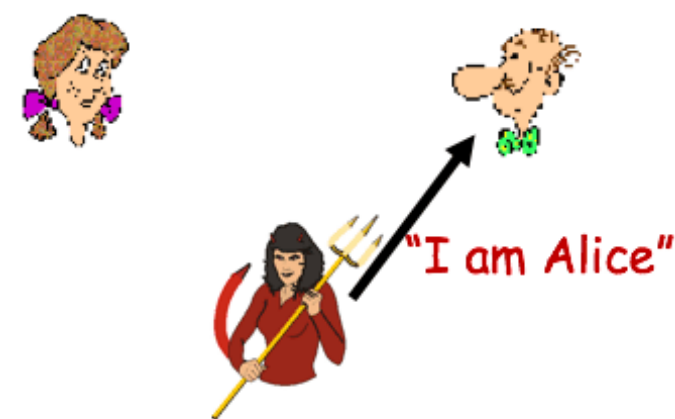
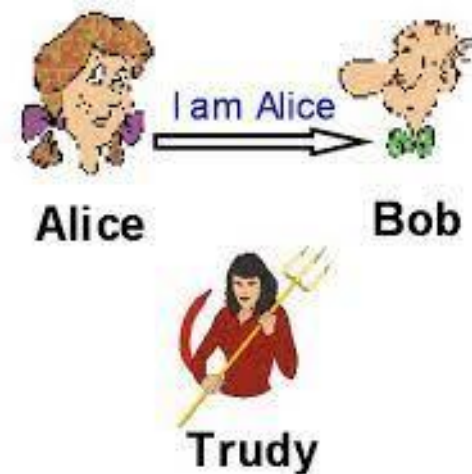
CPS REPOSITORY

Key Resources for Certificate Policies and Practices



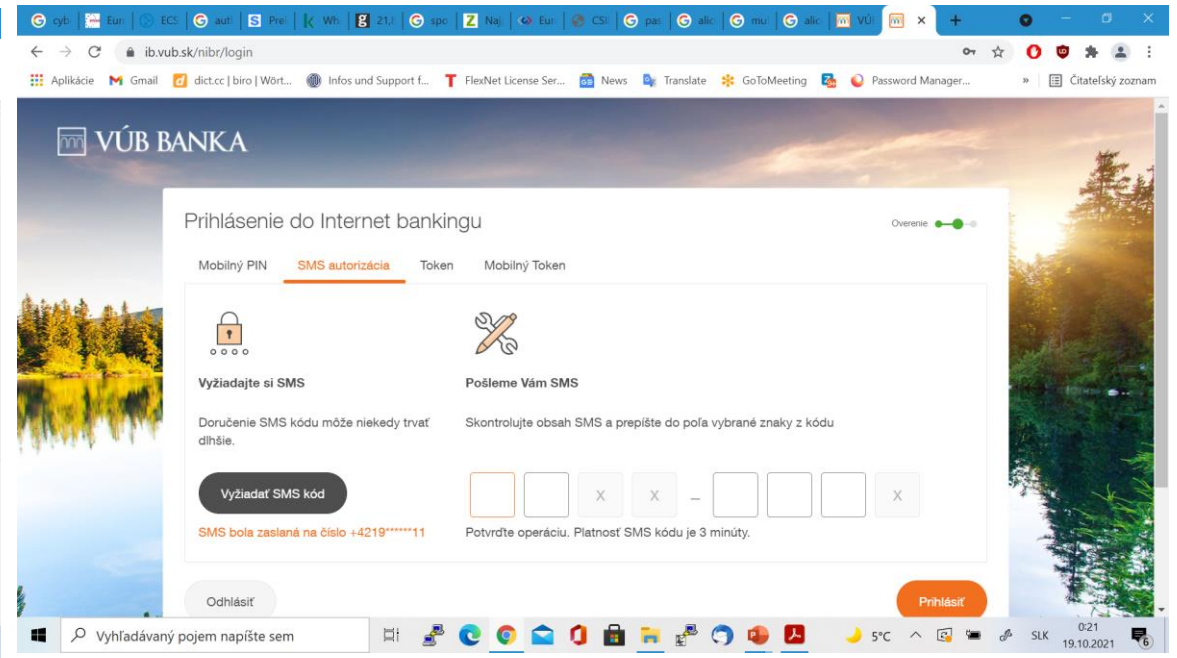
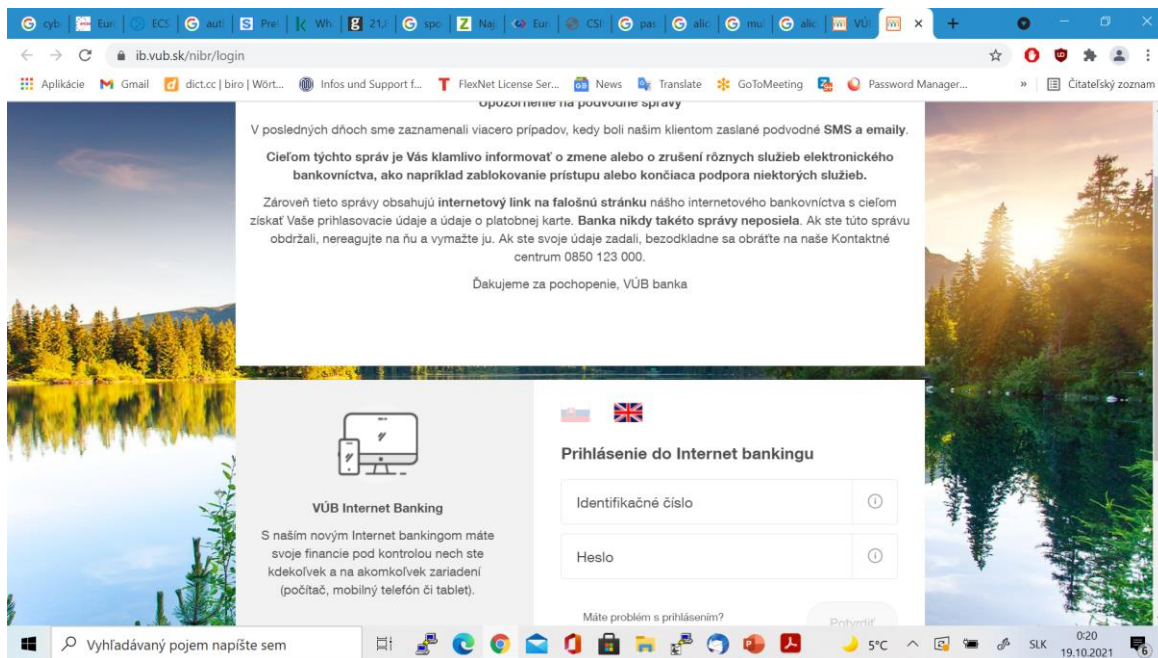
Man in the Middle útok

- Pri slabej autentifikácii môže útočník ukradnúť identifikačné údaje a vydávať sa za druhú stranu
- Ochrana – silná autentifikácia



Viacfaktorová autentifikácia

- SMS kód, token,...
- biometria



Občiansky preukaz s chipom

- **BOK - bezpečnostný osobný kód - (šesťmiestny)**
 - slúži na identifikáciu užívateľa a prístup do stránky na www.slovensko.sk,
 - dá sa zmeniť, nedá sa odblokovať
- **KEP PIN - kvalifikovaný elektronický podpis - Personal Identification Number - (šesťmiestny)**
 - slúži na podpísanie dokumentu, prihlasovacích formulárov alebo cez internet zasielaných údajov kvalifikovaným elektronickým podpisom,
 - dá sa zmeniť aj odblokovať
- **KEP PUK - kvalifikovaný elektronický podpis - Personal Unblocking Key - (osemmiestny)**
 - slúži na odblokovanie KEP PIN po jeho 3-násobnom nesprávnom zadaní,
 - dá sa zmeniť, nedá sa odblokovať

BOK V S. KEP

PREČO SA OPLATÍ MAŤ BEZPEČNOSTNÝ OSOBNÝ KÓD AJ KVALIFIKOVANÝ ELEKTRONICKÝ PODPIS



Autentifikácia

Slúži na účely overenia identity prihlasujúceho sa používateľa portálu slovensko.sk.



Osobné nastavenie

Nutná návšteva oddelenia dokladov.



Odblokovanie BOK

Používateľ si sám BOK neodblokuje.



Čo vybavím iba s BOK

Len úkony nevyžadujúce váš podpis.



Autorizácia

KEP-om môžete podpisovať a realizovať právne úkony elektronicky.



Elektronické nahratie

Vybavenie online, ak máte BOK.



Odblokovanie KEP

Používateľ si zadá KEP PUK na odblokovanie KEP-u.

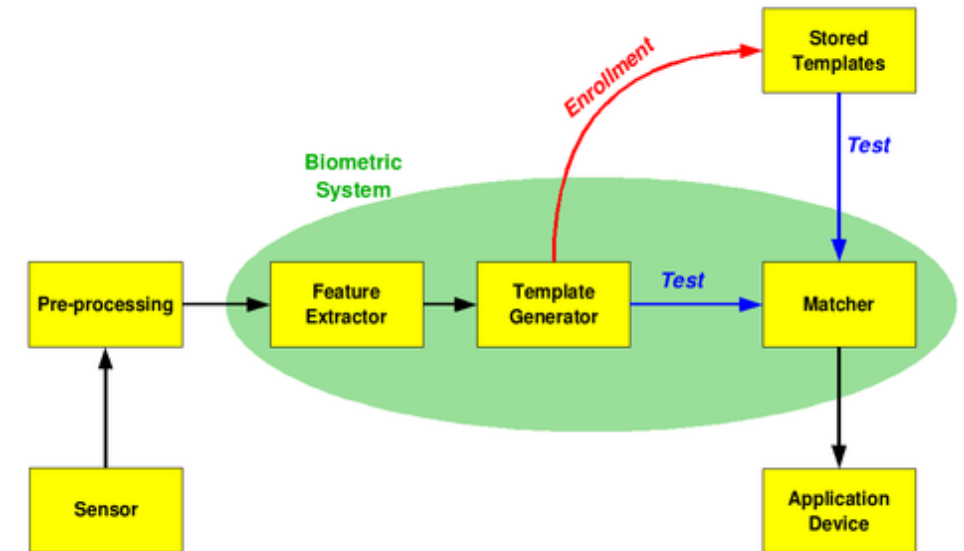
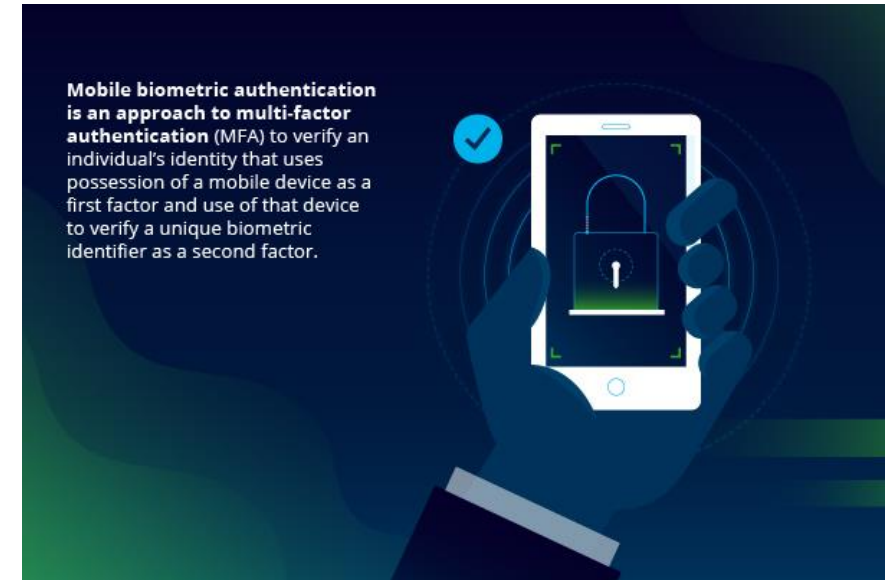


Čo vybavím s KEP

Aj úkony vyžadujúce váš úradne osvedčený podpis.

Biometrická autentifikácia

- používanie napr v autách, mobiloch
- Biometrická autentifikácia
 - Statická – otláčok prsta, retina, tvár, ušný lalok, ...
 - Dynamická – reč, písanie na klávesnici, ...
 - Podpora systémov umelej inteligencie (neurónové siete, hlboké učenie)



Mysli predtým
ako klikni!

Ďakujem za pozornosť!



Are you a robot?



I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)

