

UPUTA ZAPOSLENICIMA ZA KIBERNETIČKU SIGURNOST



10 osnovnih pravila sigurnog korištenja informacijskih sustava

Radi zaštite podataka, korisničkih računa i informacijskih sustava Fakulteta.

svi zaposlenici dužni su pridržavati se sljedećih pravila:



1. Čuvajte svoje korisničke podatke

Korisničko ime i lozinka osobni su podaci za pristup sustavima i ne smiju se dijeliti s drugim osobama. Koristite snažne lozinke i višefaktorsku autentifikaciju (MFA) kada je dostupna.



2. Provjerite poruku prije otvaranja poveznice ili pritvika

Budite posebno oprezni s neočekivanim porukama, zahtjevima za unos lozinke, promjenu računa za plaćanje ili hitnim zahtjevima. Ako niste sigurni, ne otvarajte sadržaj.



3. Ne unosite lozinku preko poveznice iz sumnjive poruke

Prije prijave provjerite mrežnu adresu stranice. Ako postoji sumnja da je riječ o lažnoj stranici, zatvorite je i pristupite sustavu na uobičajeni način.



4. Zaključajte računalo kada se udaljavate

Čak i pri kratkom napuštanju radnog mjesta zaključajte računalo. Ne ostavljajte dokumente i podatke dostupnima neovlaštenim osobama.



5. Službene podatke čuvajte samo na odobrenim mjestima

Osobne, studentske, kadrovske, financijske i druge službene podatke ne šaljte na privatne adrese elektroničke pošte i ne pohranjujte ih u neodobrene servise u oblaku.



6. Ne instalirajte programe bez potrebe i odobrenja

Na službena računala ne instalirajte neproverene, nelicencirane ili privatne programe i dodatke koji nisu potrebni za obavljanje poslova.



7. Redovito ažurirajte uređaje

Ne odgađajte sigurnosna ažuriranja operacijskog sustava, preglednika i drugih aplikacija. Ažuriranja uklanjaju poznate sigurnosne ranjivosti.



8. Oprezno koristite USB uređaje i vanjske medije

Ne priključujte nepoznate USB uređaje i druge prijenosne medije na službena računala. Povjerljive podatke ne prenosite na nezaštićenim uređajima.



9. Posebno pazite pri radu izvan Fakulteta

Službeno računalo i dokumentaciju čuvajte od krađe i neovlaštenog pristupa. Pri korištenju javnih Wi-Fi mreža budite dodatno oprezni.



10. Svaki sumnjivi događaj odmah prijavite

Odmah prijavite sumnjivu elektroničku poruku, gubitak uređaja, sumnju na neovlašten pristup računu, zlonamjerni program ili neuobičajeno ponašanje računala.



Dogodio se incident? Odmah prijavite.

Odmah prijavite:

- sumnjivu poruku ili pokušaj krađe lozinke
- slanje podataka pogrešnoj osobi
- gubitak ili krađu službenog uređaja
- sumnju da je netko pristupio vašem korisničkom računu
- pojavu zlonamjernog programa ili neuobičajeno ponašanje računala



Ne pokušavajte samostalno 'popravlјati' sigurnosni incident niti ga prešućivati. Brza prijava može znatno smanјiti posljedice.



Sigurnosni događaj ili incident prijavlјuje se ustrojstvenoj jedinici Fakulteta nadležnoj za informatičko-računarske poslove.



Kontakt: it@fzz.unist.hr | Mobitel: 099 484 28 80