



34. posvet

# Poslovanje z nepremičninami

15. in 16. november 2023

Gospodarska  
zbornica  
Slovenije 

Zbornica za poslovanje  
z nepremičninami



# Zagotavljanje kibernetске varnosti v organizaciji

Božidar Dajčman



## Božidar Dajčman

---

- direktor varnosti v večji slovenski banki
- 25+ let v finančni industriji
- Različne vloge znotraj in zunaj IT
- CISO od 2014
- CSO od 2017
- Nepremičnine?



# Agenda

---

Kaj se nam lahko zgodi?

---

Kako se lotimo zagotavljanja varnosti?

---

Koraki upravljanja varnosti

---

Vloge pri zagotavljanju varnosti

---

Nekaj namigov

---



# Kaj se nam lahko zgodi?



Vabilo Za namene sodne preiskave  
(členi 227-22, 227-22-1, 227-23 in 227-24 zakonika o kazenskem postopku)

**PREDMET: SODNI POSTOPKI**  
**NATINF: OTROŠKA PORNOGRAFIJA**  
**KIBERNETSKI PROSTOR: INTERNET**  
**SKLIC NA POSTOPEK: 09656101560/2022**



Sem **gospa TATJANA BOBNAR**, generalna direktorica slovenske policije v sodelovanju s Centralno direkcijo Evropskega policijskega urada (EUROPOL).

Kmalu po zaplembi kibernetске infiltracije bomo proti vam sprožili pravni postopek za : **Otroška pornografija, pedofilija, kibernetска pornografija in ekshibicionizem.**



Nova AI aplikacija za zaslužek s trgovanjem osvaja Slovenijo



**Končno na našem trgu. Naravni pripravek, ki izboljšuje sluh in je največji sovražnik tinitusa in vnetja ušes.**



**23-letna milijonarka iz Ljubljane pripoveduje, kako je postala bogata**

**ZAPOSILITEV** Ali potrebujete zakonit posojilo za plačilo dolga ali ustanoviti podjetje? **0** povvedb

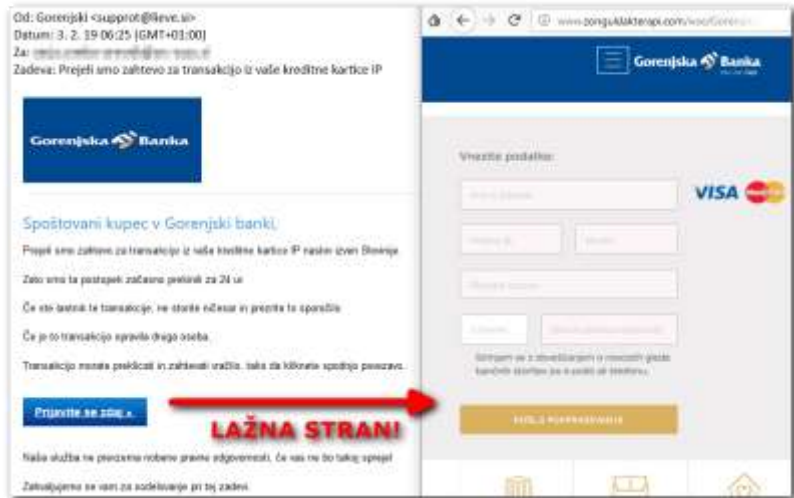
od Peter Leo v Oskrba in pomoč na domu

dober dan

Ali potrebujete zakonit posojilo za plačilo dolga ali ustanoviti podjetje če da vzpostavi stik s tem e-pošto: peterioanhome3@yahoo.com z naslednjimi podatki pod imenom: ..... Država: ..... članica ..... Znesek posojila: ..... Loan Trajanje Telefonska številka: ..... Spol: ..... Mesečni dohodek ..... hvala

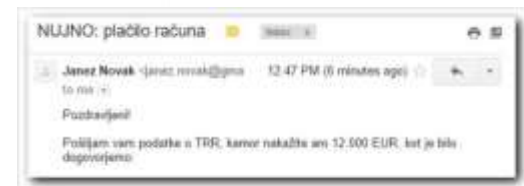
# Prevare „low-tech“

# Prevare z uporabo nekaj tehnologije



From: [Uwix Admin <UwixAdmin@voicesthief.com>](mailto:UwixAdmin@voicesthief.com)  
Date: Tuesday, October 10, 2023 at 11:13 AM  
Subject: Password Expiry NOTIFICATION

You don't often get email from [UwixAdmin@voicesthief.com](mailto:UwixAdmin@voicesthief.com), just why this is important.



Update 9.2.2022 ob 2.30: Vzdrževalna dela so zaključili.

## POP TV hekerski napad / kibernetiski napad

9.2.2022 popoldne, dan po hekerskem napadu, so na POP TV / Pro Plus podali nekaj več pojasnil.

” Celotnega obsega napada še ne moremo oceniti, trenutno smo vse svoje sile usmerili v to, da bodo naši glavni sistemi v najkrajšem času postavljeni v prvotno delovanje, kar bo omogočilo nemoteno delovanje televizijskih programov in spletnih strani.



# Kibernetski napadi



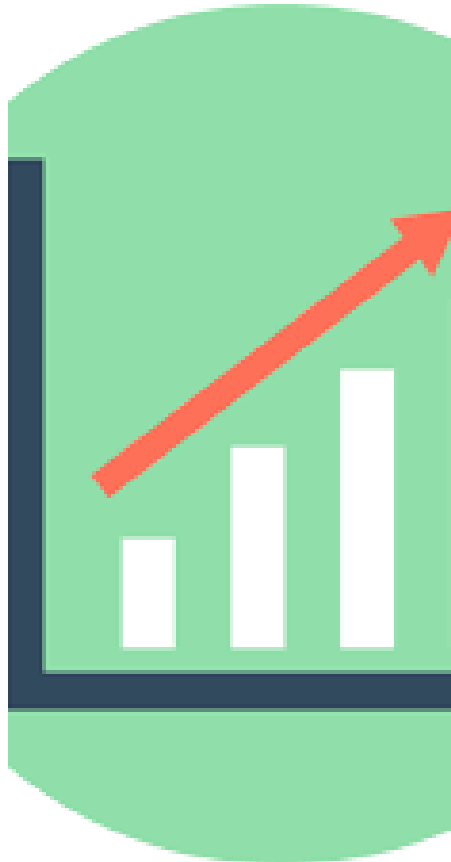
# Kolikšna je škoda?

SI-CERT: Poročilo o kibernetiki varnosti za leto 2022

Oškodovanje	Opis
 <b>najvišja oškodovanja</b>	
<b>3.000.000 EUR</b>	Najvišji znesek, na srečo neuspešnega, oškodovanja v letu 2022 (šlo je za vrivanje v poslovno komunikacijo, ang. business email compromise oz. BEC fraud) – prenos denarja je bil pravočasno zaustavljen zaradi nadzornih mehanizmov bank in Urada RS za preprečevanje pranja denarja.
<b>400.000 EUR</b>	Najvišje oškodovanje fizične osebe (izsiljevanje z lažnimi grožnjami o pregonu).
 <b>povprečna oškodovanja</b>	
58.000 EUR	Povprečno oškodovanje v nigerijski prevari (vnaprejšnje plačilo).
31.000 EUR	Povprečno oškodovanje v ljubezenski prevari.
19.000 EUR	Povprečno oškodovanje zaradi lažne tehnične pomoči Microsofta.
3.400 EUR	Povprečno oškodovanje pri phishing napadu (zloraba kreditne kartice).
780 EUR	Povprečno oškodovanje pri spletnem nakupovanju.

# Kako se lotimo zagotavljanja varnosti - izhodišča?





**Svet okoli nas**



# Kaj morajo voditelji varnosti vedeti odločevalci v organizaciji?

Security project management	New business initiatives	Fostering the culture of security	Incident preparation	SOC design - in-house	Integrating security in SDLC	Cloud infrastructure security	Business continuity planning	Regulatory
Current state assessment and improvement	New initiative identification and engagement	Campaign planning and management	Stakeholder engagement (Board, IT, HR, Legal, Communications / Marketing / Media Relations, customers, suppliers)	Recruitment Development, retention and promotion Knowledge retention Team and shift management Continuous training Technology upgrade	Secure application development standards Secure coding training and review Security pairing / 1:1 coaching Security testing in the pipeline Checking for vulnerable dependencies Checking for secrets in code	Identity and access management Configuration hardening Networking and communication security Logging and monitoring capability DDoS prevention capability Backup capability	Business impact assessment Cyber attack scenario planning Business continuity plan development and review Backup and restoration capability	Regulation Self-assessment Annual Review Supplier Control and review Improvement development implementation
Activity planning	Security consulting for Enterprise projects	Security awareness Targeted training 1:1 coaching	Stakeholder engagement (Board, IT, HR, Legal, Communications / Marketing / Media Relations, customers, suppliers)	SOC design - outsourced / MSP / shared	Product security	Container security	Endpoint security	Data protection
Supplier onboarding	Supporting internal projects	Security awareness Targeted training 1:1 coaching	Stakeholder engagement (Board, IT, HR, Legal, Communications / Marketing / Media Relations, customers, suppliers)	Supplier selection and management Contract negotiation Knowledge transfer Resource commitments Metrics and KPIs	Threat modelling Application assessment and hardening Change and configuration management	Vulnerability identification and remediation Security policies Identity and access management Network segmentation Secrets management Logging and monitoring	Asset management Secure baseline Hardening Patching / software updates Malware prevention Threat detection Encryption PIN / Password enforcement Remote wipe functionality BYOD security	GDPR support GDPR Privacy Assessment Data transfer and security
Progress tracking and reporting	Operating model	Security awareness Targeted training 1:1 coaching	Stakeholder engagement (Board, IT, HR, Legal, Communications / Marketing / Media Relations, customers, suppliers)	Alerting from security tools Log analysis and correlation Open source and commercial threat feeds Threat hunting (automated and manual) Social media and Dark Web monitoring	Security testing and assurance	Security operations	Supply chain	Security audit
Coordinating product security improvements	Operating model	Security awareness Targeted training 1:1 coaching	Stakeholder engagement (Board, IT, HR, Legal, Communications / Marketing / Media Relations, customers, suppliers)	Identity repository and federation Credential and password management Multifactor authentication Joiners movers leavers HR process integration Process review	Integrating security testing in the QA process Code reviews Penetration tests / red team exercises Bug bounty / vulnerability disclosure programme Continuous security testing	Anomaly detection capability Procedures and runbooks Rule adjustments Metrics and KPI reporting SOC and ticketing system Investigation	Pre-contract due diligence New contract review Contract renewal Negotiations SLAs	Security audit
Governance	Operating model	Security awareness Targeted training 1:1 coaching	Stakeholder engagement (Board, IT, HR, Legal, Communications / Marketing / Media Relations, customers, suppliers)	Cyber insurance	Email security	Team		
Information Security Management System	Roles and responsibilities	Data security	Incident notification strategy Incident coordination and response tooling	24x7 security monitoring Identification Triage Containment Resolution Recovery Root cause analysis and lessons learned Digital forensics capability	Anti-spam controls Email encryption Malware protection Phishing protection SPF, DKIM & DMARC			
Policy and procedure development and review	Checklist management	Data security	Incident notification strategy Incident coordination and response tooling	Broker and underwriter engagement Limits and deductibles Covered scenarios Pre-breach risk and control maturity assessment				
Roles, responsibilities and ownership	Finance	Data security	Incident notification strategy Incident coordination and response tooling					
Risk management	Aligning with investment portfolio	Data security	Incident notification strategy Incident coordination and response tooling					
Risk assessment	Budgeting and tracking	Data security	Incident notification strategy Incident coordination and response tooling					
Risk ownership and governance	Investor relations (funding, governance, etc.)	Data security	Incident notification strategy Incident coordination and response tooling					
Risk articulation and management review	Mergers and acquisitions	Vulnerability management	Incident notification strategy Incident coordination and response tooling					
Risk mitigation strategy	Risk management Due diligence Secure integration	Vulnerability management	Incident notification strategy Incident coordination and response tooling					
Risk acceptance	Physical security	Vulnerability management	Incident notification strategy Incident coordination and response tooling					
Process	Physical security	Vulnerability management	Incident notification strategy Incident coordination and response tooling					
Tooling for risk management / risk log maintenance	Physical security	Vulnerability management	Incident notification strategy Incident coordination and response tooling					
Merging risk identification	Physical security	Vulnerability management	Incident notification strategy Incident coordination and response tooling					
Brand protection	Physical security	Vulnerability management	Incident notification strategy Incident coordination and response tooling					
Marketing and	Physical security	Vulnerability management	Incident notification strategy Incident coordination and response tooling					

# Odločanje na podlagi strahu?

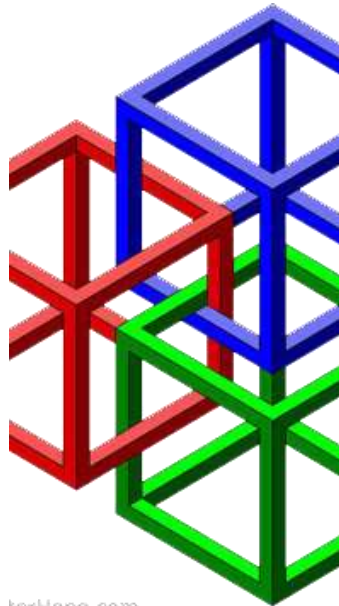


**Odločanje  
na podlagi  
nadzora  
tveganj!**



# Koraki upravljanja varnosti





terHope.com



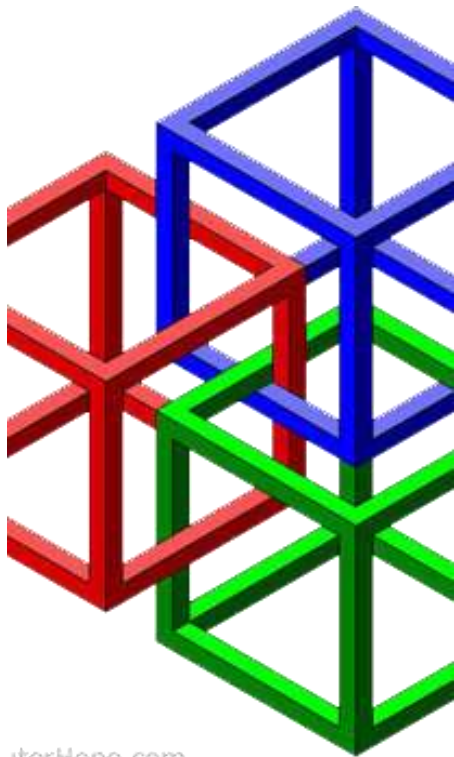
**Kje smo?  
Kam hočemo?**





**Komunikacija**

# Okvir upravljanja varnosti

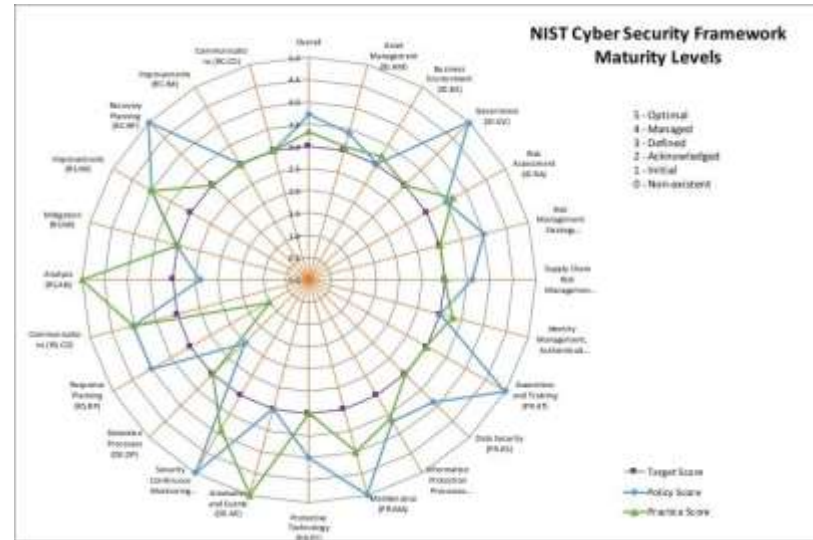
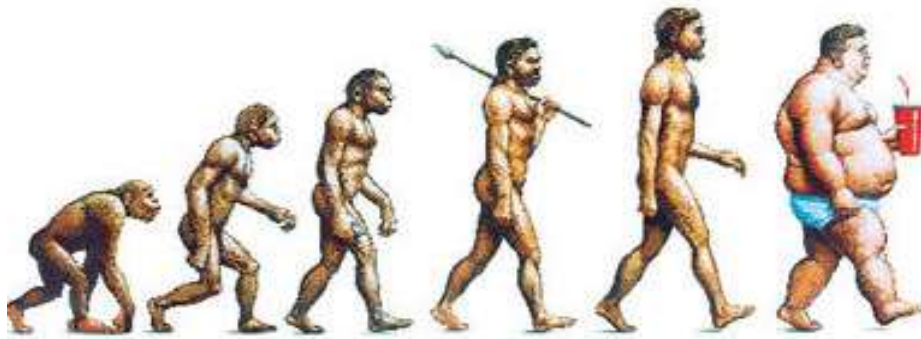


sterHope.com



**Three lines of defence**

# Stopnja zrelosti



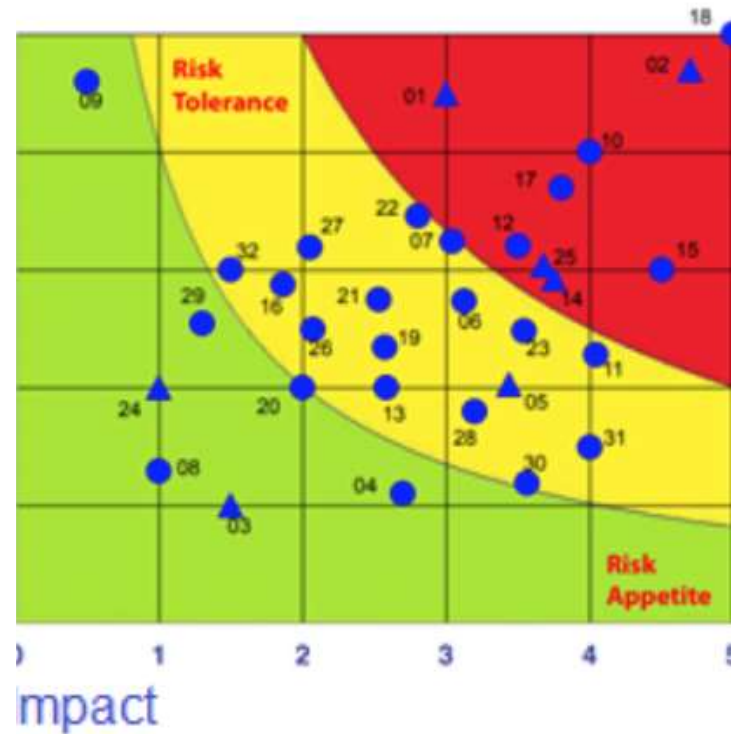
	Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
<b>People</b>	Activities unstaffed or uncoordinated	Infosec leadership established, informal communication	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
<b>Process</b>	No formal security program in place	Basic governance and risk management process, policies	Organization-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
<b>Technology</b>	Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement

- |  |  |  |   |   |
|--|--|--|---|---|
| <p><b>LEVEL 1</b><br/>Initial</p> <ul style="list-style-type: none"> <li>Minimal cyber awareness</li> <li>Minimal cyber info sharing</li> <li>Minimal cyber assessments and policy &amp; procedure evaluations</li> <li>Little inclusion of cyber into Continuity of Operations Plan (COOP)</li> </ul> | <p><b>LEVEL 2</b><br/>Established</p> <ul style="list-style-type: none"> <li>Leadership aware of cyber threats, issues and imperatives for cyber security and community cooperative cyber training</li> <li>Informal info sharing/communication in community; working groups established; ad-hoc analysis, little fusion or metrics; professional orgs established or engaged</li> <li>No assessments, but aware of requirement; initial evaluation of policies &amp; procedures</li> <li>Aware of need to integrate cyber security into COOP</li> </ul> | <p><b>LEVEL 3</b><br/>Self-Assessed</p> <ul style="list-style-type: none"> <li>Leaders promote org security awareness; formal community cooperative training</li> <li>Formal local info sharing/cyber analysis, initial cyber-physical fusion; Informal external info sharing/ cyber analysis and metrics gathering</li> <li>Autonomous tabletop cyber exercises with assessments of info sharing, policies &amp; procedures, and fusion; routine audit program; mentor externals on policies &amp; procedures, auditing and training</li> <li>Include cyber in COOP; formal cyber incident response/recovery</li> </ul> | <p><b>LEVEL 4</b><br/>Integrated</p> <ul style="list-style-type: none"> <li>Leaders and orgs promote awareness; citizens aware of cyber security issues</li> <li>Formal info sharing/analysis, internal and external to community; formal local fusion and metrics, initial external efforts</li> <li>Autonomous cyber exercises with assessments of formal info sharing/local fusion; exercises involve live play/metrics assessments</li> <li>Integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery</li> </ul> | <p><b>LEVEL 5</b><br/>Vanguard</p> <ul style="list-style-type: none"> <li>Awareness a business imperative</li> <li>Fully integrated fusion/analysis center, combining all-source physical and cyber info; create and disseminate near real world picture</li> <li>Accomplish full-scale blended exercises and assess complete fusion capability; involve/mentor other communities/entities</li> <li>Continue to integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery</li> </ul> |
|--|--|--|---|---|

P-DRP	M	L	M
Control & governance	M	M	M
on incomplete/incorrect	H	M	H
e provider	H	L	M
utsource provider	H	L	M
	H	L	H
ersonnel / experience	H	H	H
	H	L	M
ayment from client	L	L	L
	M	L	M
ownturn	M	M	M
lan	H	L	H
	H	M	H
	M	H	L
	H	L	M

Impact Rating	Likelihood Rating	Inherent Risk
M	L	M
M	M	M
H	M	H
H	M	H
H	L	M
H	L	M
H	L	H
H	H	H
H	L	M
L	L	L
M	L	M
M	M	M
H	L	H
H	M	H
M	H	L
H	L	M

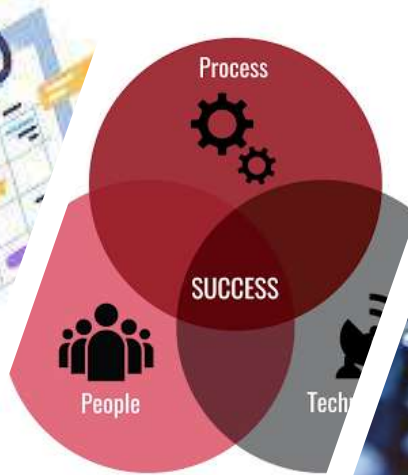
Control Assessment	Residual Risk
S	L
S	L
S	M
S	M
S	L
S	L
S	L
MOD	H
MOD	H
MOD	M
S	L
S	L
S	L
S	M
MOD	H
S	L
S	L



M, L = Low, S = Satisfactory, MOD = Moderate, W = Weak



# Ocena tveganj



# Strateško in taktično načrtovanje

# Vloge pri zagotavljanju varnosti





**Kdo je zadolžen za kibernetško varnost v organizaciji?**

## Vloge pri kibernetski varnosti

- Vse zaposleni
- Strokovne službe
- Vodstvo organizacije





# MANAGED SECURITY PROVIDERS CAN DELIVER:



**Kaj namesto nas  
lahko naredijo  
drugi?**

- MSSP (managed security service providers)
- **Odgovornosti ne moremo prenesti, zato je razumevanje kibernetских tveganj potrebno znotraj organizacije.**

# Nekaj namigov



# Ozaveščenost zaposlenih!

SI-CERT (nacionalni odzivni center)

[www.varninainternetu.si](http://www.varninainternetu.si)

[www.varnivpisarni.si](http://www.varnivpisarni.si)



**VARNI**  
v pisarni

Učni moduli Moj račun ▾

• BREZPLAČNI SPLETNI TEČAJ ZA ZAPOSLENE

## 30 minut za informacijsko varnost na delovnem mestu

En sam napačen klik lahko pomeni neznansko škodo za podjetje. Z brezplačnim tečajem boste pridobili novo znanje, kako ostati vami v pisarni. Tečaj opravite kadarkoli, vsebine prilagodite svojim delovnim nalogam.



# Začnite pri začetku



- Upravljanje informacijskih sredstev
- Omejene dostopne pravice
- Požarna pregrada
- Zaščita pred zlonamernimi programi
- Nameščanje varnostnih popravkov
- Avtentikacija
- Varnostne kopije
- ...

**Zagotovite si  
neodvisno  
mnenje**



# Pripravite se na incident!

- Koga boste poklicali?
- Kdo bo sprejemal odločitve?
- Kako boste komunicirali z javnostjo in nadzornimi institucijami?
- Kako boste okrevali po napadu?

# Hvala za pozornost.

