

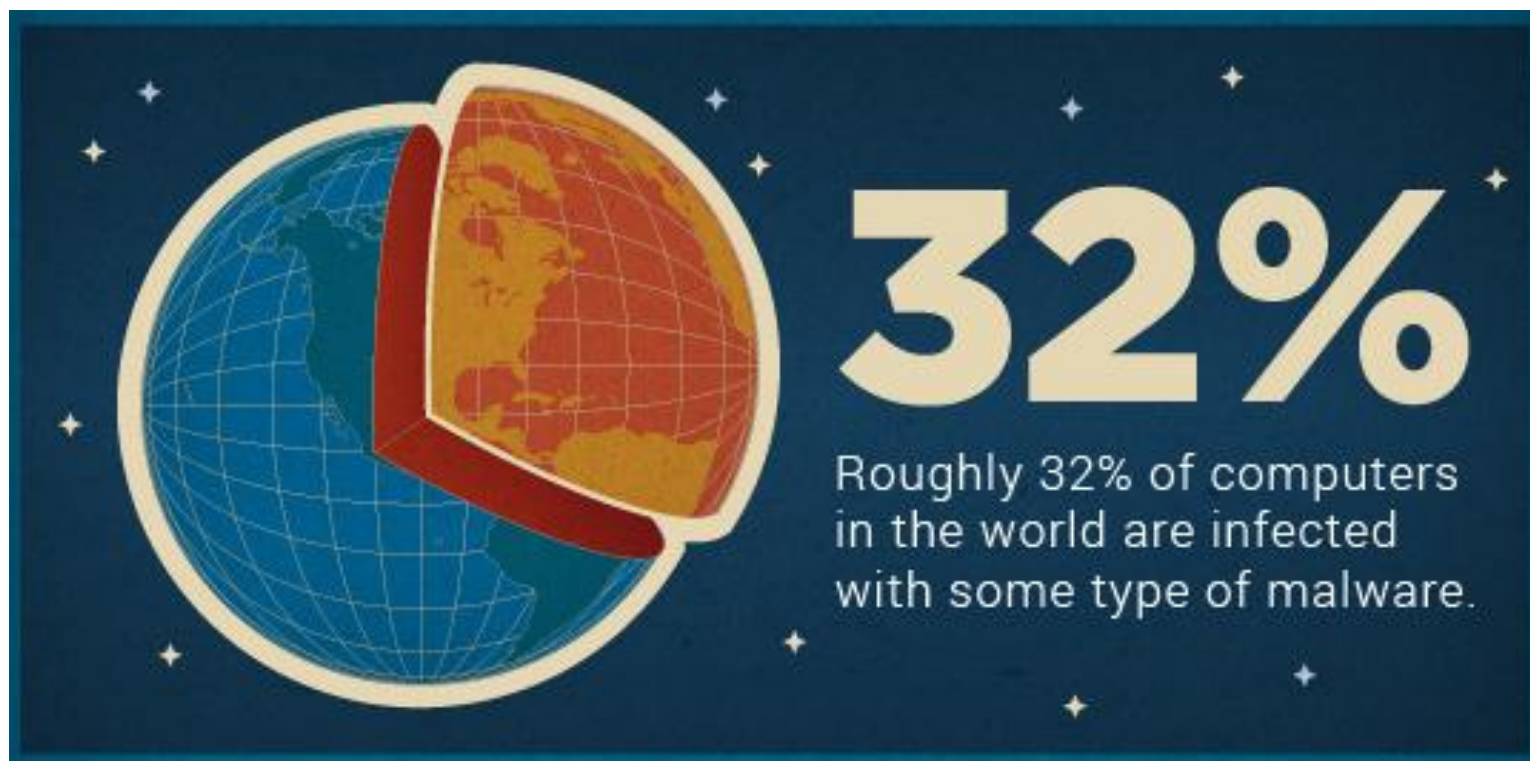


Internetna varnost

Kako zagotoviti varnost uporabnikov in podatkov pred škodljivimi vplivi z interneta

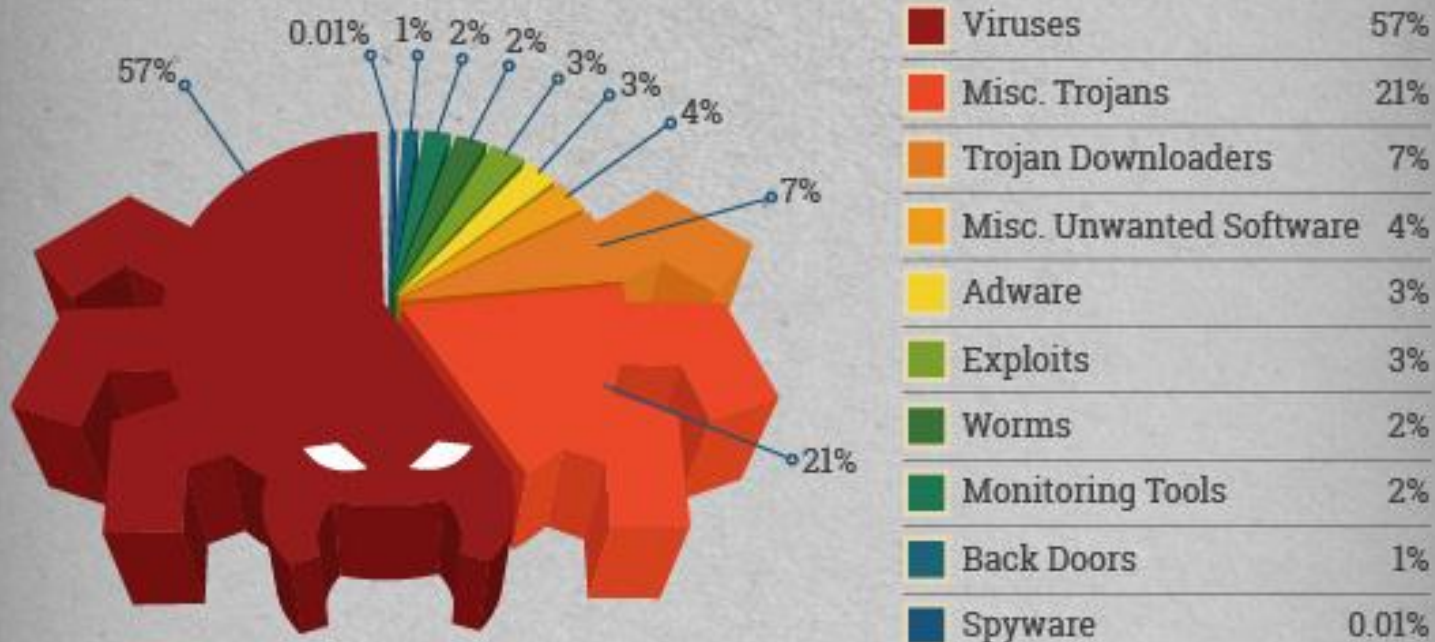


STATISTIKA



STATISTIKA

What are we *Infected* with?





STATISTIKA

There were approximately **27 Million** strains
of malware created last year.



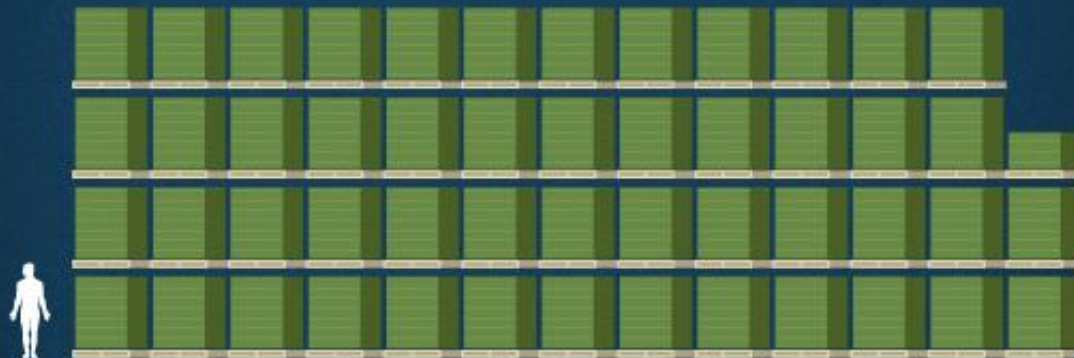
That's **74,000** new viruses every day.



STATISTIKA

How much do viruses *Cost* us?

\$4.55 BILLION



Here's what \$4.55 Billion U.S. Dollars looks like in pallets full of stacked \$100 notes. That's the estimated cost to U.S. households per year from viruses, spyware and other malware.



STATISTIKA

Social media

a hackers' favorite
target

600.000

Facebook accounts are compromised every single day

Hackers use out of date versions to launch attacks

99%



of computers
are vulnerable
to exploit kits

Social engineering

Cyber criminals' favorite way to manipulate victims





Kako se naš rač. lahko okuži ?

- Največ okužb s preprostim brskanjem po spletu,
- uporaba slabih gesel (ista gesla za več programov/storitev), ki niso dovolj močna,
- $\frac{3}{4}$ vseh Malware in računalniških virusov se širi preko socialnih omrežij.

- Virusi, malware in spyware se največkrat širijo ne skozi napake v programski opremi, ki nam služi kot varnostni mehanizem pred njimi, vendar skozi človeško napako.

- Večina ljudi je slišala, da naj ne odpirajo priponk v e-sporočilih, klikajo povezav za katere ne vedo kaj so. Prav tako je večina ljudi slišala, da je potrebno redno telovaditi in jesti zdravo. Pa vendarle se te smernice večkrat ne upoštevajo.

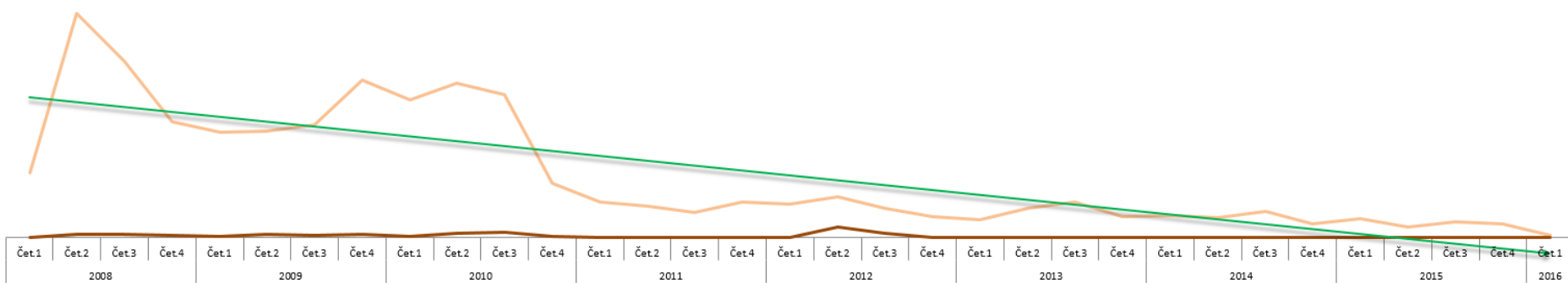
The biggest secret to why computers keep getting infected is that people don't follow basic best practices, and that's not really a secret at all to security professionals.

— Jonathan Sander, strategy & research officer

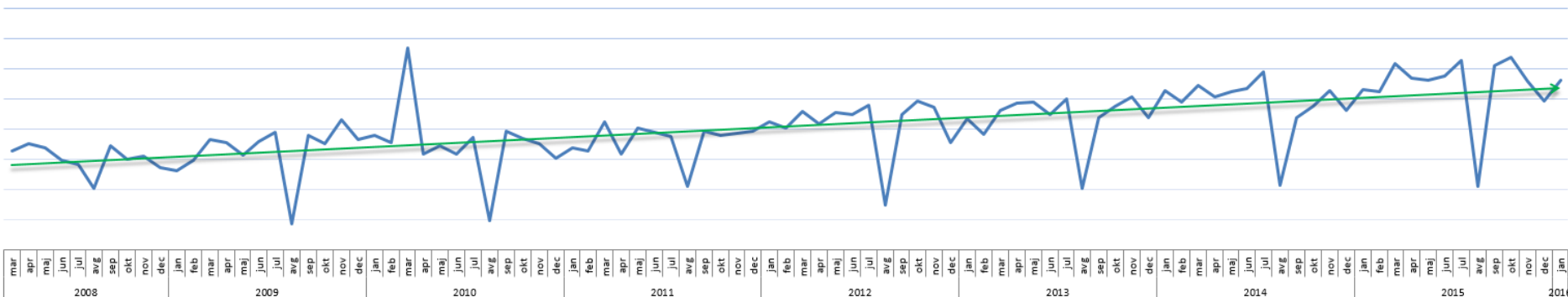


Največ okužb po e-pošti ?

Delež neželjene e-pošte:

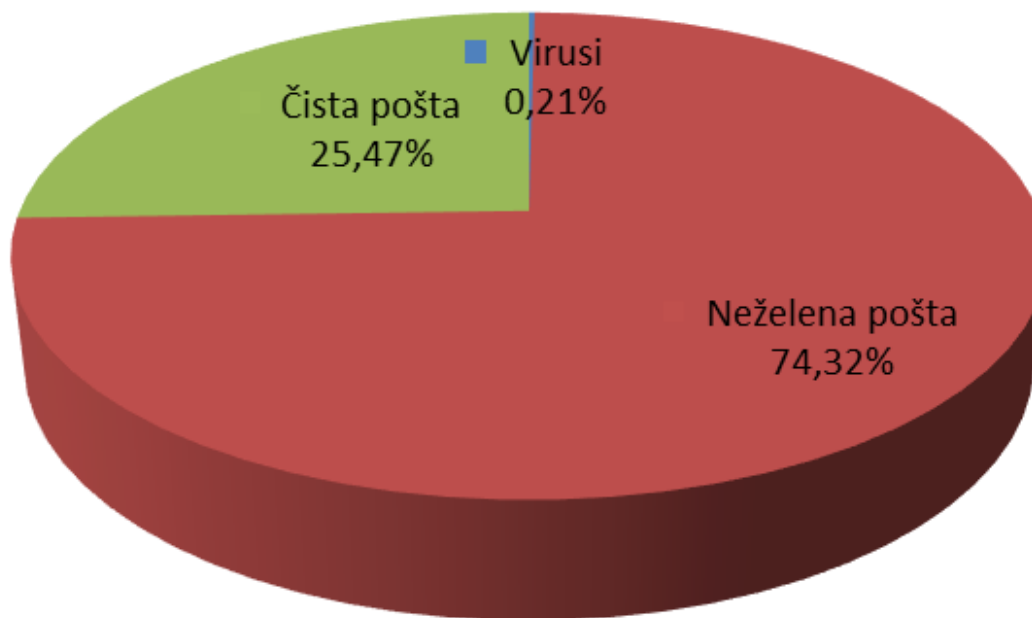


Delež željene e-pošte:



Največ okužb po e-pošti ?

Klasifikacija pošte





■ Virusi ■ Neželena pošta ■ Čista pošta



Osnovna zaščita pred grožnjami

- Ozaveščanje uporabnikov (<https://www.varninainternetu.si/>, <http://www.safe.si/>),

Ime ▲	Datum spremembe	Tip	Velikost
 Posvet_PDBI_Internetna_Varnost	28.2.2016 17:55	Bližnjica	2 KB
 Posvet_PDBI_Internetna_Varnost.pptx.exe	28.2.2016 15:42	Program	1.265 KB

Awariness!

- kompleksna gesla,
- dobre varnostne kopije ključnih podatkov,
- požarni zid na vhodu internetne povezave v podjetje,
- posodobljen protivirusni program,
- posodobljeni operacijski sistem z zadnjimi varnostnimi posodobitvami,
- posodobljena uporabniška programska oprema (Adobe Flash, Java),
- ...



Osnovna zaščita pred okužbami v e-sporočilih

The screenshot shows an Outlook email header for 'GZDBK <info@gzdbk.si>' with the subject 'Novoletno voščilo'. A yellow warning bar at the top states: 'Kliknite tukaj, če želite prenesti slike. Outlook je zaradi zaščite vaše zasebnosti preprečil samodejni prenos določenih slik v tem sporočilu.' Below this, a white box contains a warning: 'Če želite prenesti slike, kliknite z desno tipko miške ali tapnite in pridržite prst tukaj. Outlook je preprečil samodejni prenos slik iz interneta, da bi zaščтил vašo zasebnost. Gospodarska zbornica Dolenjske in Bele krajine'. The email body contains the text 'Novoletno voščilo' followed by another warning: 'Če želite prenesti slike, kliknite z desno tipko miške ali tapnite in pridržite prst tukaj. Outlook je preprečil samodejni prenos slik iz interneta, da bi zaščтил vašo zasebnost.'

Ključ do uspeha:

Ustrezna ozaveščenost uporabnikov!

The screenshot shows an email body with a blue URL: http://www.telekom.de/x/kundencenter?wt_mc=abrechnungen_Rechnung_festnetz. A white warning box above the URL contains the text: 'http://thammyhongngoc.vn/ygvpsla48vi' and 'Kliknite za sledenje povezavi'. At the bottom, a header area shows: 'Received: from webby.t-media.si (webby.t-media.si) by ... with ESMTTP id AADE67DA896 for ...'.



Dodatna zaščita pred grožnjami

- Ozaveščanje in konstantno! izobraževanje IT varnostnih specialistov,
- spremljanje trenutnih groženj (<https://www.cert.si/si/obvestila/>),
- spremljanje novičarskih strani za internetno varnost za IT varnostne specialiste ([SOPHOS Naked Security](#), [Kaspersky ThreatPost](#), [InfoSEC](#), ...),
- kompleksna gesla in rotiranje gesel,
- dobre varnostne kopije ključnih podatkov, tudi “offline” kopije na več lokacijah,
- dostop uporabnikov do spleta samo skozi posredniški strežnik (proxy),
- požarni zid tudi za komunikacijo uporabnik -> splet,
- sistem za zaznavanje in preprečevanje vdorov (IDS, IPS),
- v kolikor je WiFi z dostopom do interneta v podjetju, le-ta fizično ločen od lokalnega omrežja podjetja,
- penetracijski test (angl. Penetration test), ugotavljanje varnostnih pomankljivosti,
- ...

Izsiljevalski kripto virusi (CryptoLocker)

Imam posodobljeno protivirusno zaščito ...

Tradicionalni požarni zidi in protivirusni programi delujejo na principu programskih prstnih odtisov in obnašanj. Niso zmožni detektirati in preprečiti neznanih groženj!

Moje datoteke so kriptirane, kaj pa sedaj ?

- plačajte in dobili boste nazaj datoteke, brez plačila ni možno dekriptirati datotek





HVALA ZA POZORNOST

