Informatika

Predavanje

Bezbednost računarskih sistema

Zaštita od virusa - Informacija.rs

ija.rs

(no subject) - fikana... | Prirodna kozmetika:... | Academy387 Saraje... | Microsoft dataset ai... | Security and privac... | Higher Education |...

Informacija
Saznajte više o računarskoj bezbednosti

VESTI | TEKSTOVI O ZAŠTITI | ANTI-SPAM | OPISI VIRUSA | REČNIK | OSTALE VESTI | MOBILNI TELEFONI | DRUŠTVENE MREŽE | SAJBER HRONIKA

Izdvajamo: Informacija.rs na Facebook-u | Informacija.rs na Twitter-u | Pratite nas preko RSS-a

Upišite termin pretrage | Traži

Bag u WhatsAppu korišćen za instalaciju špijunskog softvera na iPhone i Android uređajima

Mobilni telefoni, 15.05.2019.

WhatsApp je ispravio sigurnosnu grešku (CVE-2019-3568) u aplikaciji koja omogućava instalaciju špijunskog softvera na Android i iPhone uređajima.

Sigurnosni propust u planetarno popularnoj aplikaciji koja korisnicima nudi end-to-end enkripciju, omogućio je napadačima da instaliraju izraelski špijunski softver na pametnim telefonima, bez interakcije korisnika, i to samo pomoću običnog WhatsApp poziva.

Za iskorišćavanje baga bio je dovoljan WhatApp poziv i manipulacija paketima podataka poslatim kada se poziv pokrene. Korisnici čak nisu morali ni da odgovore na poziv, jer bi se zlonamerni kod... Dalje »

Prijavite se na našu mailing listu i primajte najnovije vesti (jednom dnevno) putem emaila svakog radnog dana besplatno:

vaš@e-mail | Prijava

Izdvojeno

Informacija.rs od sada prilagođena ekranima mobilnih uređaja

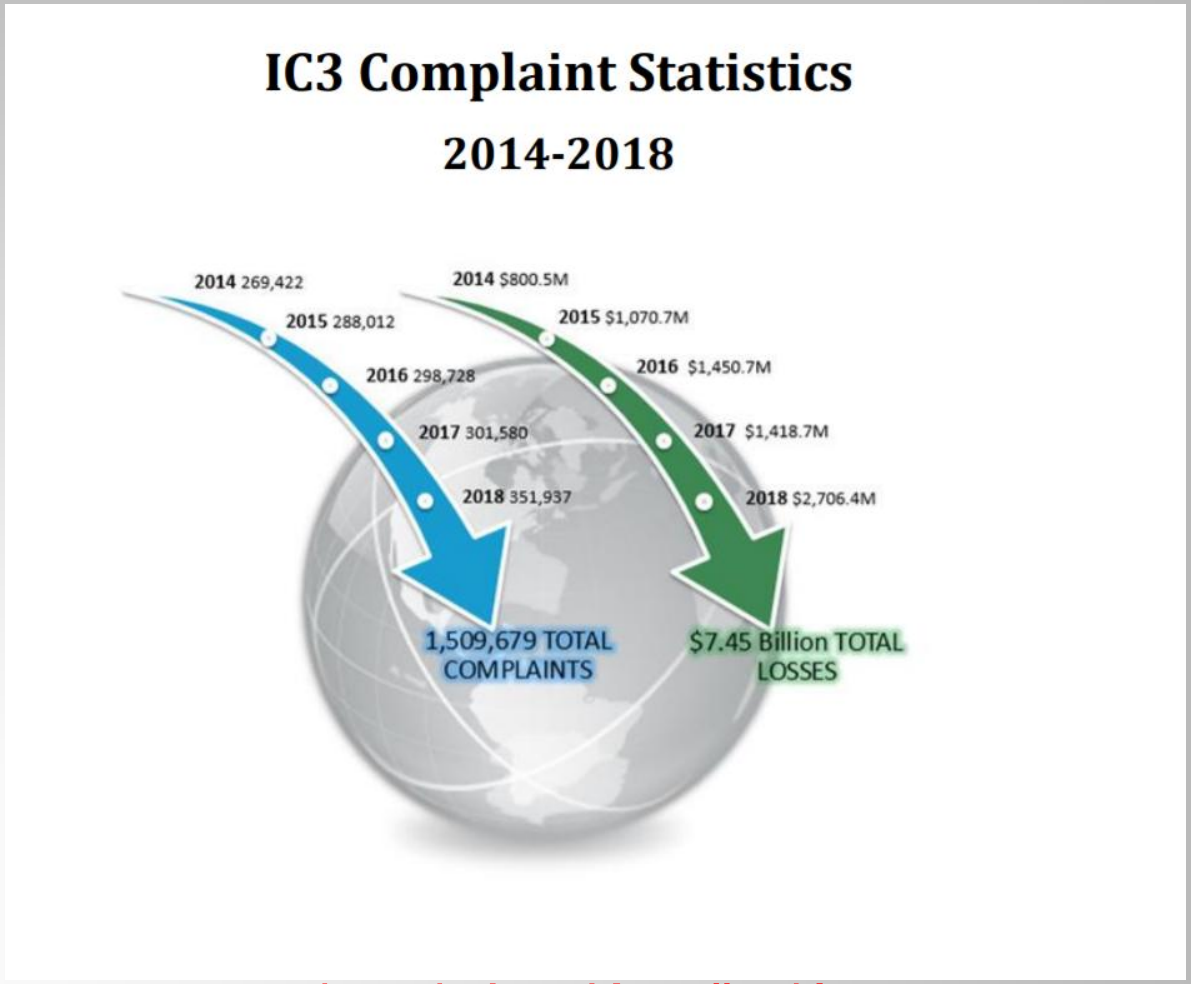
Jedna lepa vest za naše redovne čitaoce - Informacija.rs je

Ekonomske posledice sajber kriminala

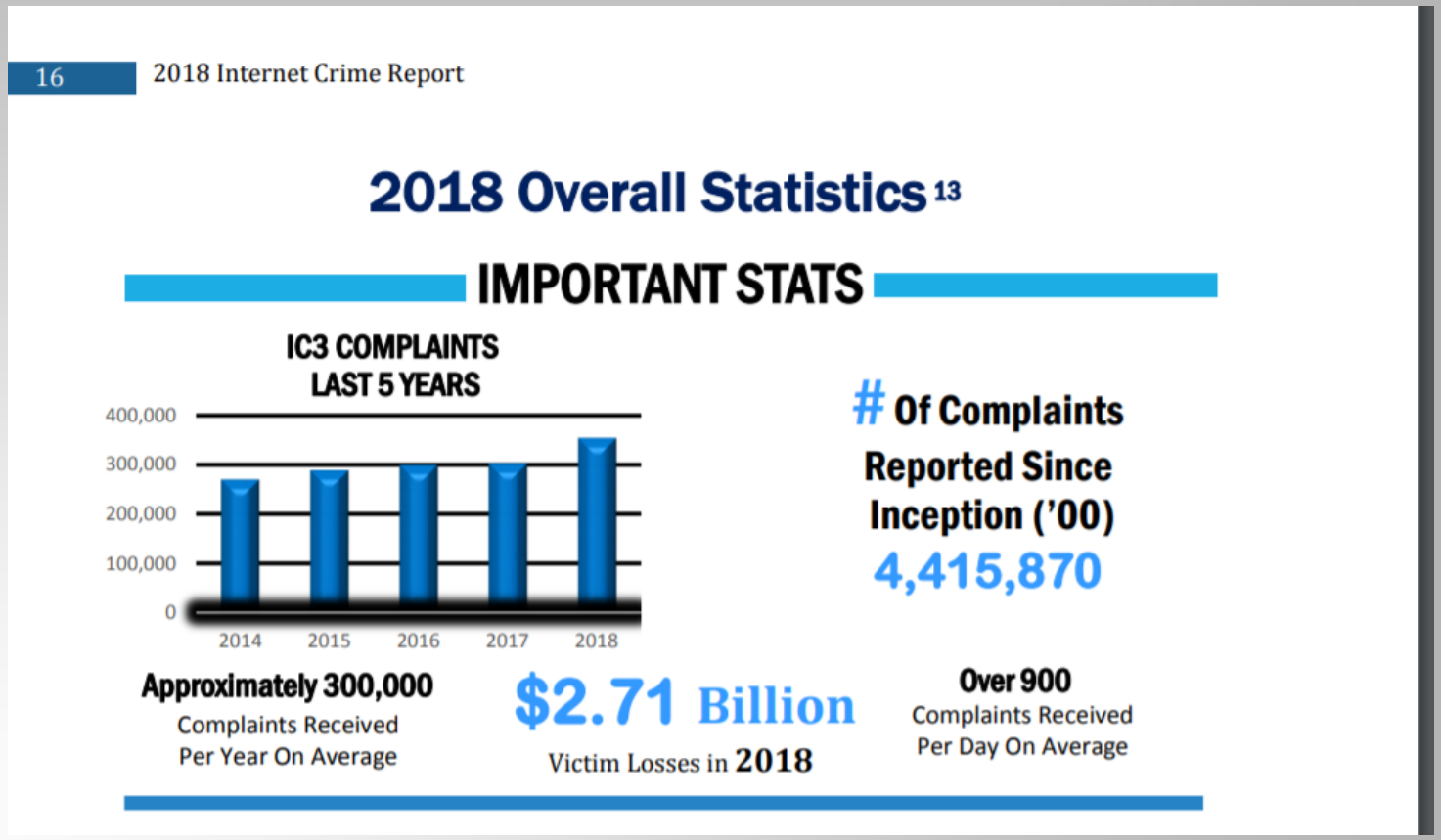
- 2014: *SC Magazine: sajber kriminal i ekonomska špijunaža koštaju globalnu ekonomoju više od $445 milijardi godišnje.(Easttom: Computer security fundamentals, 2016)*

Prema Pricewaterhouse Coopers, 2015 je otkriveno 38% incidenata više nego 2014, i 56% povećanje intelektualnog vlasništva.

Internet Crime Complaint Center (IC3) www.ic3.gov



Internet Crime Complaint Center (IC3) www.ic3.gov



Internet Crime Complaint Center (IC3) www.ic3.gov

2018 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Non-Payment/Non-Delivery	65,116	Other	10,826
Extortion	51,146	Lottery/Sweepstakes	7,146
Personal Data Breach	50,642	Misrepresentation	5,959
No Lead Value	36,936	Investment	3,693
Phishing/Vishing/Smishing/Pharming	26,379	Malware/Scareware/Virus	2,811
BEC/EAC	20,373	Corporate Data Breach	2,480
Confidence Fraud/Romance	18,493	IPR/Copyright and Counterfeit	2,249
Harassment/Threats of Violence	18,415	Denial of Service/TDoS	1,799
Advanced Fee	16,362	Ransomware	1,493
Identity Theft	16,128	Crimes Against Children	1,394
Spoofing	15,569	Re-shipping	907
Overpayment	15,512	Civil Matter	768
Credit Card Fraud	15,210	Charity	493
Employment	14,979	Health Care Related	337
Tech Support	14,408	Gambling	181
Real Estate/Rental	11,300	Terrorism	120
Government Impersonation	10,978	Hacktivist	77

Descriptors*

Social Media	40,198	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	36,477	

Krađa identieta

- Krađa identiteta: krađa ličnih podataka kao što su ime, adresa, datum rođenja, JMBG, bankovini račun i informacije o kreditnoj kartici.
- Mnoge žrtve krađe identiteta provode mesece, ili čak godine, pokušavajući da poprave kredit i eliminišu lažni dug.

Sajber kriminal

- Krađa kompjuterske opreme **NIJE** sajber kriminal.

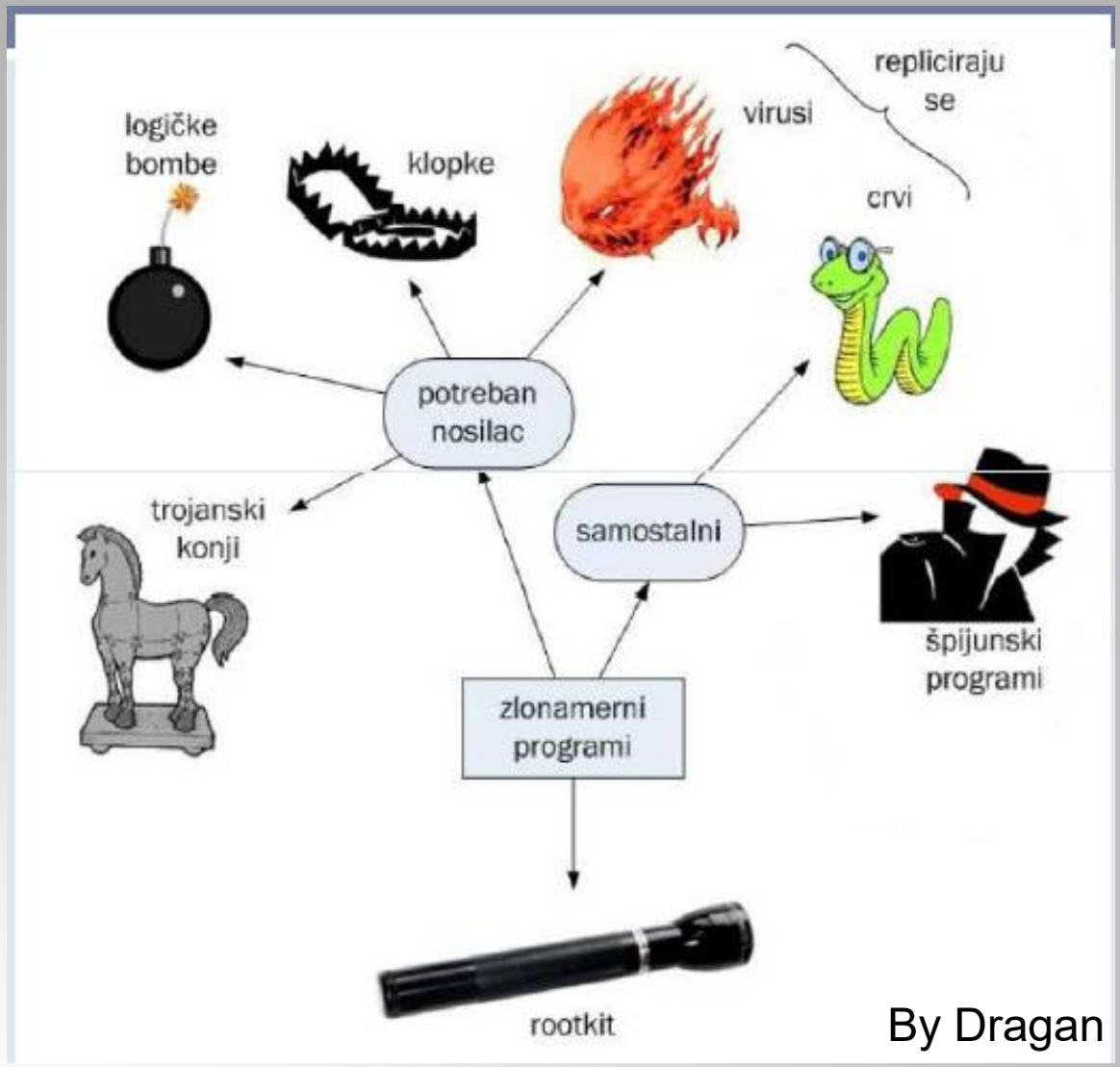
- Krađa kompjuterske opreme:
  - U porastu
  - Cena polovne robe je visoka i može se prodati online

ZLONAMERNI PROGRAMI

Zlonamerni programi

Različite posledice:

- narušavanje performansi sistema
- “neobično” ponašanje sistema
- preusmeravanje zahteva za otvaranje Web stranica
- praćenje aktivnosti i uznemiranjanje korisnika
- krađa ili uništavanje poverljivih informacija
- izvršavanje DoS napada na određeni server
- isključivanje sigurnosnih aplikacija
- menjanje podataka u bazi Registry
- oštećenje hardvera i dr.



By Dragan Pleskonjić, 2010.

Virus

- Kompjuterski virus: Program koji se “prikači” za drugi kompjuterski program.
- Širi se na druge kompjutere razmenom fajlova
- Najrasprostranjeniji tip sajber kriminala.
- Neki prouzrokuju samo manja uznemiravanja, dok drugi prave destrukciju ili kradu podatke.

Virus

- Glavna svrha
  - Replicira se i kopira što može više.
- Sekundarni cilj
  - Usporava mreže
  - Prikazuje uznemiravajuće poruke
  - Uništava fajlove ili sadržaj hard diska

Virusi

- Ukoliko je računar izložen zaraženom fajlu, virus će pokušati da se kopira i inficira fajl na računaru.
- Izvori infekcije virusa:
  - Dowloadovanjem inficiranog fajla (muzika/video)
  - Korišćenjem fleša na kome je zaraženi fajl
  - Downloadovanje ili izvršavanje fajla zakačenog za e-mail.

Virusi

IZVOR: Alan Evans, Kendall MartinMary, Anne Poatsy: Technology In Action, 2014

Skript i makro virusi

- Neki virusi se skrivaju na websajtu u formi skripta.
  - Skript je mini programa koji se izvršava bez znanja korisnika.
- Makro virusi se kače za dokumet (npr. Excel, Word) koji koristi makro viruse.
  - Makro je kratka serija komandi koje obično izvršavaju ponavljajuće zadatke.

Virusi

- E-mail virusi
  - *Mellisa virus*: prvi praktični primer e-mail virusa
  - Koriste *address book* za distribuiranje virusa.
- **Boot-sektor virus** se često prenosi preko fleša ostavljenog u USB portu. Kad se kompjuter pokrene sa spojenim flešom, kompjuter pokušava da pokrene *master boot-record*

Virusi enkripcije (Encription viruses)

- Kada je računar zaražen virusima enkripcije, oni izvršavaju programe koji traže uobičajene tipove fajlova podataka (npr. kao MS Word ili Excel fajlove) i kompresuju ih koristeći kompleksne ključeve enkripcije koji čine time fajlove neupotrebljivim.
- Nakon toga ucena: traži se novac za dekripciju programa.
- (RANSOMWARE)

Virusi

- Virusi se mogu klasifikovati prema metodama koje koriste da ih ne bi otkrio antivirusni (AV) softver:
  - **Polimorfni virusi:** Menjaju svoj kod (ili periodično prepišu preko delova) da bi izbegli detekciju. Većina polimorfnih virusa inficira jedan određeni tip fajlova (npr. EXE).
  - **Multipartite virusi:** inficira više tipova fajlova sa ciljem da zavara AV softver šta traži.
  - **Nevidljivi (stealth) virusi:** brišu privremeno njihov kod sa hard diska i prebacuju se u RAM. Na ovaj način AV ih neće otkriti ako pretražuje samo hard disk.

Logičke bombe bombe

- Logičke bombe (i vremenske) bombe
  - Logičke bombe: okidaju se kad određeni logički uslovi se zadovolje.
  - Vremenske bombe: okidaju se prolaskom vremena ili za određeni datum.

Crv (Worm)

- Crv
  - Replicira **se sam bez ljudske intervencije** širi se preko e-mail-a i/ili mreže.

  Napomena: Virusu je potrebna ljudska intervencija za širenje.

ZAŠTITA POMOĆU AV SOFTVERA

Sprečavanje infekcije virusa

- Antivirusni (AV) softver je kreiran za otkivanje virusa i zaštitu kompjutera.
- Primeri AV kompanija:
  - Symantec
  - Kaspersky
  - AVG
  - McAfee
- Složeni *Internet security* paketi vas štite od drugih pretnji.

Prvencija infekcije virusa pomoću AV softvera

- Iako AV softver je kreiran da otkrije sumnjive aktivnosti svo vreme, trebalo bi da se ceo sistem skenira jednom nedeljno.
- Ukoliko se sumnja na problem, odmah skenirati računar.
- Moderni AV skeniraju sistem u pozadini kad CPU nije previše opterećen; a može se podesiti da se skenira kada se ne koristi računar (npr. kada je u sleep modu).

Prvencija infekcije virusa pomoću AV softvera

- Osnovne funkcije antivirusnog softvera
  - Detekcija: AV traži “virus siganture” u fajlu
    - Signatura virusa je deo koda virusa koja je jedinstvena za određeni virus.
  - Zaustavljanje izvršavanja virusa: Ako AV pronađe *virus signature* ili sumnjivu aktivnost (pokretanje nepoznatog makroa), prestaje izvršavanje fajla i obaveštava o otkrivanju virusa i stavlja ga u karantin.
  - Prevencija buduće infekcije
    - In inoculation, AV sofver snima ključne atribute o kompjuterskim fajlovima i čuva ovu statistiku na sigurnom mestu. Kada skenira sistem, upoređuje prethodno stanje sa novim da bi se otkrile promene.

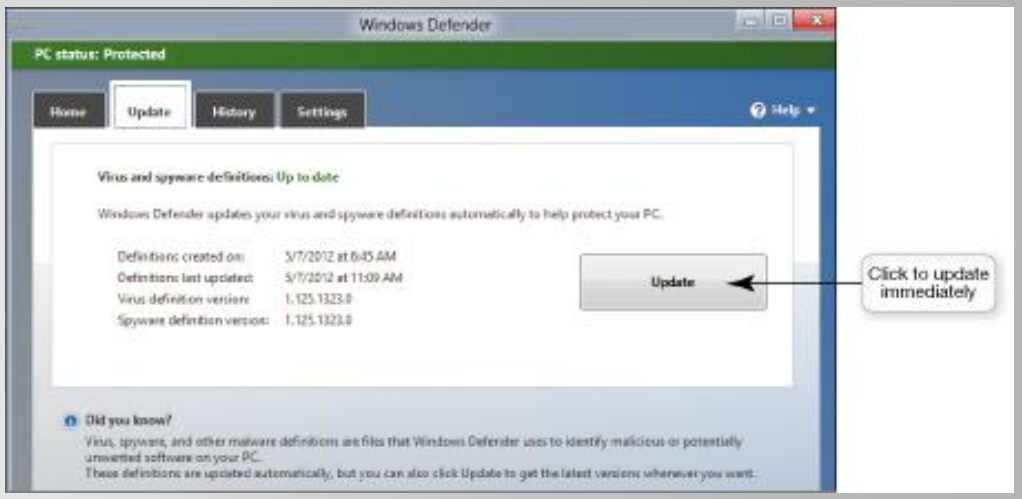
Prvencija infekcije virusa pomoću AV softvera

- Da bi se borili protiv nepoznatih virusa, programi traže sumnjive aktivnosti koje upućuju na virus, kao i signaturu virusa.
- Važno je da AV softver bude ažuriran.

Prvencija infekcije virusa pomoću AV softvera

- Većina novih kompjutera dolazi sa preinstaliranim AV softverom:
  - Obično probna verzija.

- Većina AV programa ima automatsko ažuriranje karakteristika.



AV softer za mobilne telefone

- Pametni telefoni i drugi mobilni uređaji su takođe osetljivi na viruse.
- Mnoge AV softverske kompanije nude AV za mobilne, kao npr. *Trend Micro's Mobile Security* za Android.

Prevencija infekcije virusa
Ažuriranje softvera

- Mnogi virusi koriste slabosti OS.
- Preuzimanjem malicioznog fajla sa websajta: tip napada drive-by-download, prema Google-u 1/1000
- POMOĆ: Proveriti da operativni sistem su ažurirani i da sadrže poslednje sigurnosne zakrpe (patches).
  - U Windowsu inicijalna opcija je da automatski se ažurira.
- Ažuriranje i AV softvera.

HAKERI

Hakeri

- Ko su hakeri? Nejedinstveno gledište.
- Bilo ko neželjeno upada u računarski sistem jedan računar ili mrežu.
- Tipovi hakera:
  - Etički hakeri (hakeri sa belim šeširom) – proveravaju sistem da bi otkrili ranjivosti. the Certified Ethical Hacker test (EC Council)
  - Hakeri sa crnim šeširom – upadaju u sistem da unište/modifikuju podatke ili sa nekim nelegalnim ciljem
  - Hakeri sa sivim šeširom – da bi pokazali svoje umeće ili pokušali da prodaju svoje usluge.

Hakeri

Hakeri mogu da nađu puno privatnih informacija o vama na Internetu.

Problemi koje hakeri mogu da naprave

- Krađa informacija o kreditnim i debitnim karticama koje se nalaze na hard disku.
- Upad na sajtove koje imaju informacije o kreditnim karticama.
- Na većinu sajtova je potrebno da se unese login ID i password da bi se pristupilo.
- Čak iako podaci nisu sačuvani na računaru, hakeri mogu da ih “uhvate” kada ste online korišćenjem packet analyzer-a (sniffer-a) ili keylogger-a.

Problemi koje hakeri mogu da naprave

- Podaci putuju preko Interneta u paketima, koji su identifikovani sa IP adresom, da bi se olakšalo identifikacija računara na koju su poslati. Kada paketi dostignu odredište, oni se sastavljaju u kohezivnu poruku.
- Packet analyzer (sniffer): Program su razvili hakeri koji pregledaju svaki paket.

Npr. haker dok sedi u kafiću korišćenjem paket sniffera “hvata” osetljive podatke (kao što je broj debitne/kreditne kartice) od ljudi koji koriste wireless mrežu kafića. Ovakve mreže mogu biti posebno osetljive, za ovaj tip istraživanja ako ekripcija podataka nije omogućena kada je postavljena mreža.

- Jednom kad haker ima informacije o tuđoj kartici (kreditnoj/debitnoj) mogu započeti kupovanje ili prodaju informacija nekome drugom ili imati druge osetljive podatke.
- Rešenje zaštita od packet sniffing-a instalacijom firewall-a i korišćenjem enkripcije podataka na bežičnoj mreži.

Hakeri
Trojanski konji i Rootkit

- Trojanski konj (Trojanac) izgleda da je koristan, ali dok se izvršava čini nešto zlonamerno u pozadini bez znanja vlasnika računara.
- Najčešće zlonamerna aktivnost od *trojanca* je instalacija backdoor programa ili rootkit-a.
- Backdoor (zadnja vrata) ili rootkit programi (ili grupa programma) koja omogućava hakeru da ostvari pristup računaru i preuzme potpunu kontrolu nad njim bez vašeg znanja.
- Korišćenjem backdoor programa, hakeri imaju pristup i briš sve fajlove na računaru, šalju poštu, izvršavaju programe i dr. Računar koji haker kontroliše na ovaj način je zombi.
- Zombi se često koriste da izvrše DoS (Denial-of-service) napad na drugi računar.

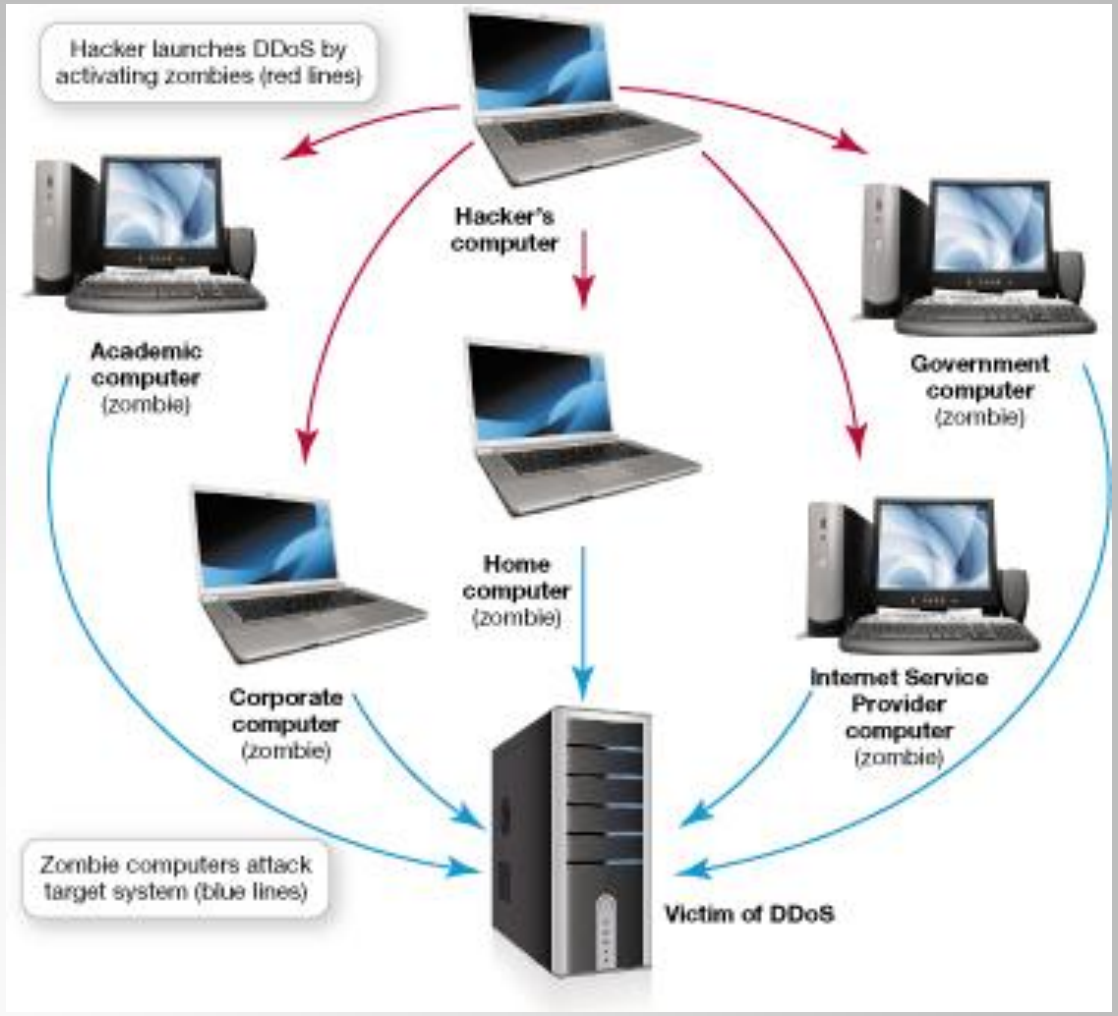
Hakeri
Denial-of-Service napad

- Prilikom napada Denial-of-service (DoS) korisnicima je uskraćen pristup kompjuterskom sistemu pošto haker iznova ponavlja zahteve tom računaru preko računara koje je on ili ona preuzeli kao zombi. Kada je preplavljen zahtevima u DoS napadu, sistem se obara i odbija da odgovori na zahteve legitimnih korisnika. (prema tome računar je zauzet “lažnim” zahtevima pa autorizovan korisnik ne može da dobije pristup.
- Izvršavanje DoS napada na kompjuterski sistem sa jednog računara od jednog korisnika je jednostavno za praćenje. Zato, većina hakere koriste distribuirani DoS, gde se izvršava DoS napada sa više od 1 zombija (nekada i hiljade zombija) u isto vreme. Hakeri kreiraju mnoge zombije i koordinišu ih tako da oni počinju da šalju “lažne” zahteve istom računaru u isto vreme.

Hakeri
Denial-of-Service napad

- Napad DDoS (Distributed denial-of-service) se izvršava sa više od jednog zombi kompjutera, što administratoru napadnutog računara onemogućava zaustavljanje napada. Često, napadi su kooridnirani automatski od strane botneta.
- Botnet je velika grupa softverskih programa (koji se zovu roboti ili botovi) koji se izvršavaju autonomno na zombi računaru. Neki botnet-ovi su imali 1.5miliona kompjutera.
- Pošto mnogi komercijalni web sajtovi imaju prihode od korisnika, direktno ili indirektno (kao što web surferi kliknu na oglase), DDoS napadi mogu biti finansijski NAPORNI za vlasnike websajtova.

Hakeri
Denial-of-Service napad



Hakeri
Kako hakeri pristupaju računaru

- Direktan pristup
  - Instaliranje softvera za hakerisanje → Rešenje: postaviti password.
- Indirektan pristup
  - Preko Internet konekcija
  - Logički portovi su virtualne komunikacioni gateway-evi ili putanje koje omogućavaju kompjuteru da organizuje zahteve za informacijama.
    - Logički portovi su brojevi dodeljeni nekom servisu. Npr. logički port 80 je za HTTP: glavni komunikacioni protokol za web
  - Rešenje: instalacija firewall-a.

OGRANIČENJE PRISTUPA DIGITALNIM RESURSIMA

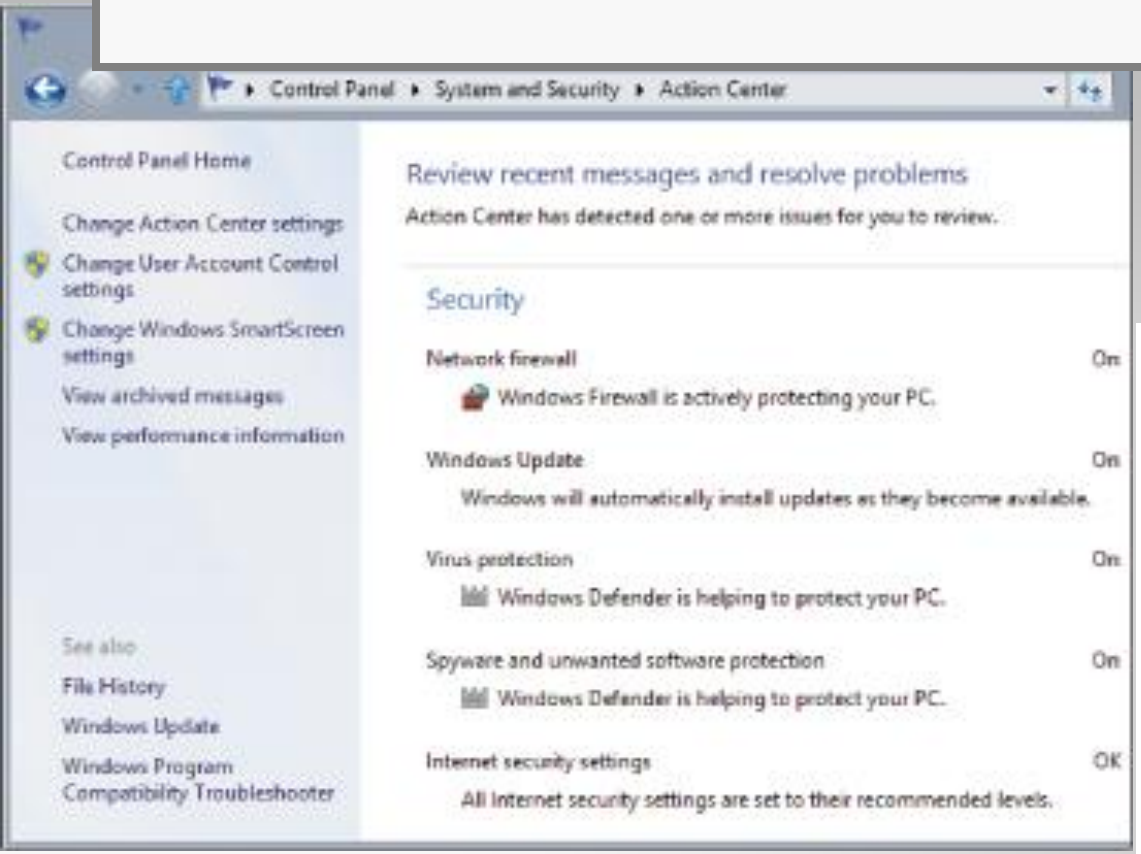
Ograničenje pristupa digitalnim resursima

- Držati podalje hakere
  - Sprečiti hakere da pristupe računaru
  - Zaštititi digitalne informacije
    - Npr. korišćenjem passworda
  - Sakriti aktivnosti od znatiželjnih

Firewalls

- Firewall: softverski program ili hardverski uređaj kreiran da zaštiti kompjutere od hakera.
- Lični firewall: specifično dizajniran za kućnu mrežu. Korišćenjem ličnog firewall-a mogu da se zatvore/otvore logički portovi za napadače i potencijalno učinite vaš kompjuter nevidljivim na druge kompjutere na Internetu.
- I hardverski i softverski firewalls će vas zaštiti od hakera. Jedan tip nije bolji od drugog, a maksimalna zaštita se postiže instaliranjem oba.

Kako radi Firewall



Windows Actiron Center prikazuje status programa koji štite tvoj kompjuter:
U Control Panelu izaberite System and Security -→ Action Center.

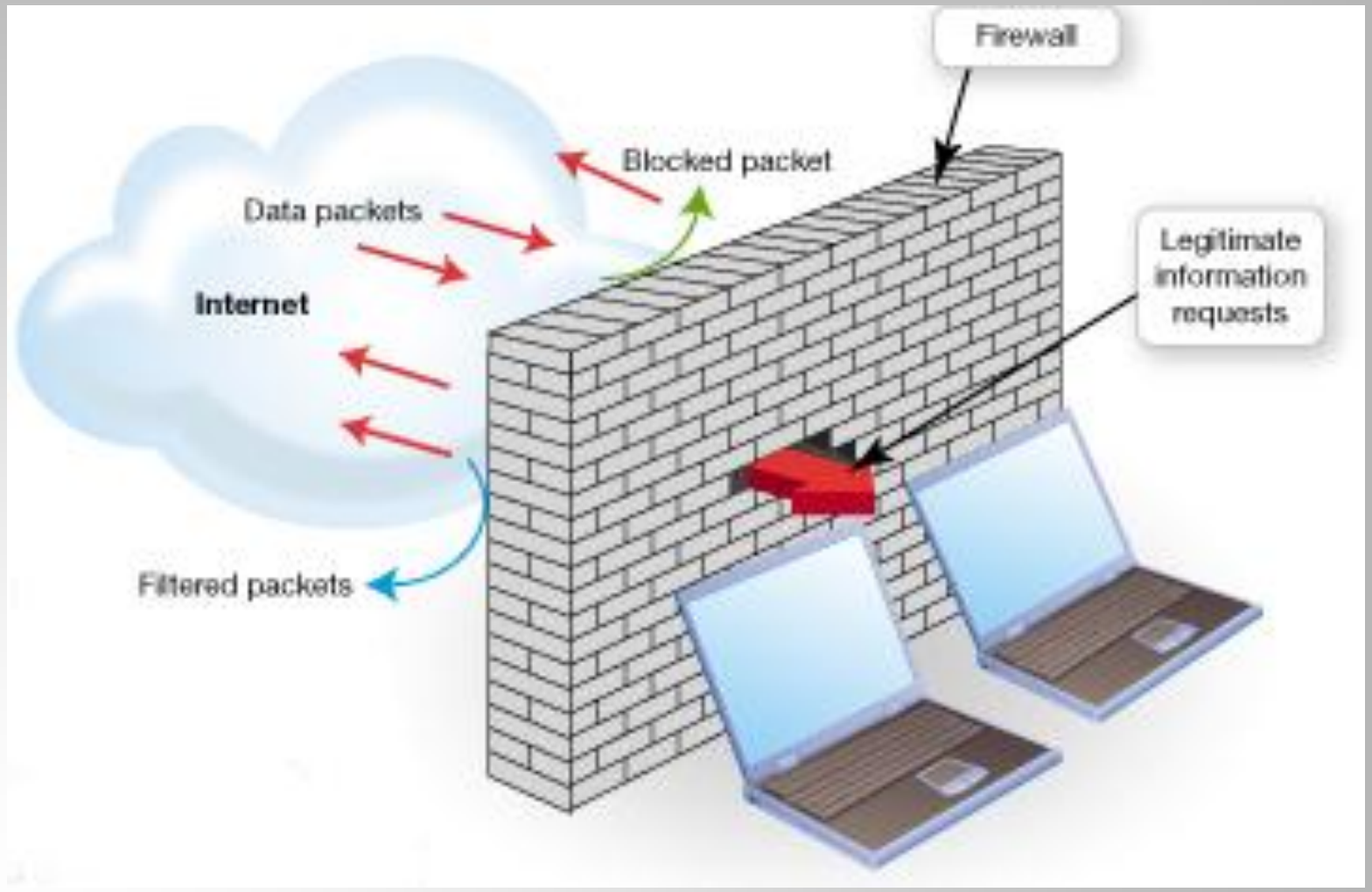
Kako radi Firewall

- Firewalls štiti na dva glavna načina:
  - Blokirajući pristup logičkim portovima
  - Čineći da je adresa kompjuterske mreže bezbedna.
- Filtriranje paketa je proces konfigurisanja firewall-a da filtrira pakete poslate logičkim portovima.

Kako radi Firewall

- **Logičko blokiranje portova**: Firewall je konfigurisana da ignoriše zahteve koji potiču sa Interneta za pristup određenim portovima.

Kako radi Firewall



Provera bezbednosti računara

- Testiranje ranjivosti računanra
  - **Gibson Research (www.grc.com)**
    - ShieldsUP
    - LeakTest
- Ako su ranjivosti otkrivene:
  - Instalirati firewall ako nemate
  - Ako je firewall već konfigurisan, proveriti kako da se zatvore ili ograniče pristupi portovima.

Provera bezbednosti računara

- Uobičajeni logički portovi

Broj porat	Protokol koji se koristi za port
21	FTP (File TransferProtocol)
23	Telnet (Unencripted text communication)
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (domain name system)
80	HTTP (Hypertext Transfer Protocol)
443	HTTPS (HTTP with Transport Layer Security [TSL] encription)

Lozinka

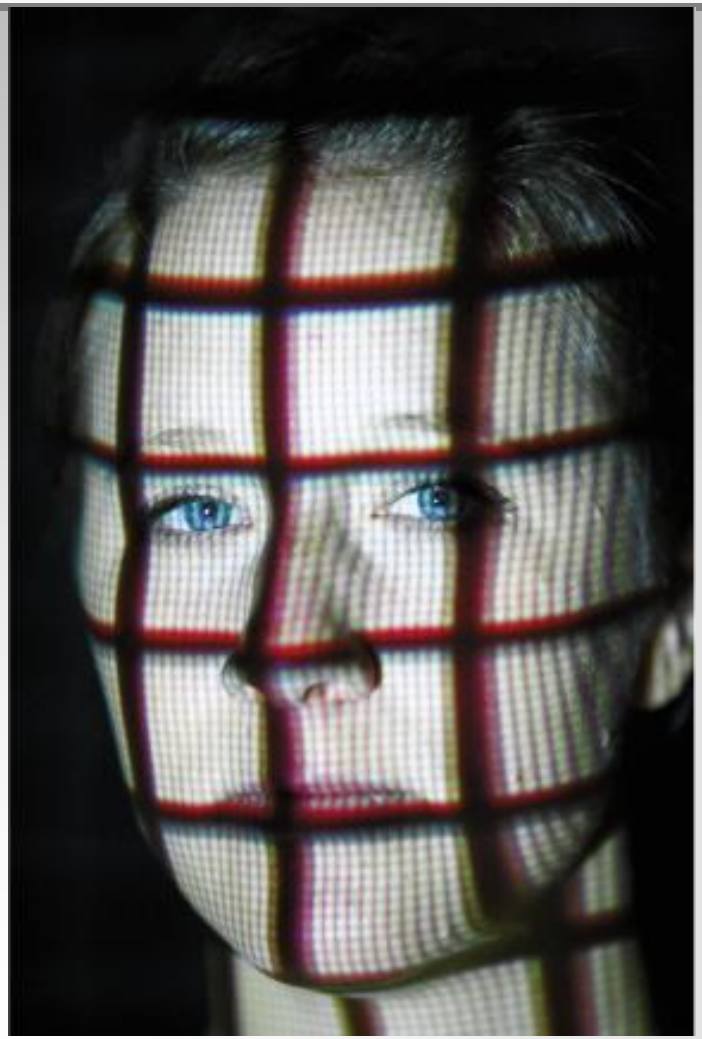
- Test za proveru jačine lozinke, npr. PasswordMeter.
- Operativni sistem ima ugrađnu zaštitu passworda.

Anonimnost na Webu

- Danas browseri (GoogleChrome, Firefox, ili Ineternet Explorera) imaju alate za privatnost koje omogućavaju pretraživanje weba anonimno:
  - Incognito, Private Browsing, InPrivate
- → Nema istorije pretraživanja, nema sačuvanih privremenih (temporary) fajlova.

Anonimnost na Webu

Uređaji za biometrijsku autentifikaciju



Softer za prepoznavanje lica je sada dostupan za laptop.

UPRAVLJANJE ONLINE UZNEMIRAVANJEM

Adware

- Adware: Softver koji prikazuje sponzorisane reklame u delu browsera ili kao pop-up prozori. Smatra se legitiman mada, ponekad uznemiravajući.
  - Browseri (Firefox, Safari, IE..) blokiraju ili smanjuju pop-up-ove.
  - Neki pop-up-ovi su legitimni i povećavaju funkcionalnost originalnog sajta.
- Može se podesiti u browseru za koje sajtove je dozvoljen pop-up

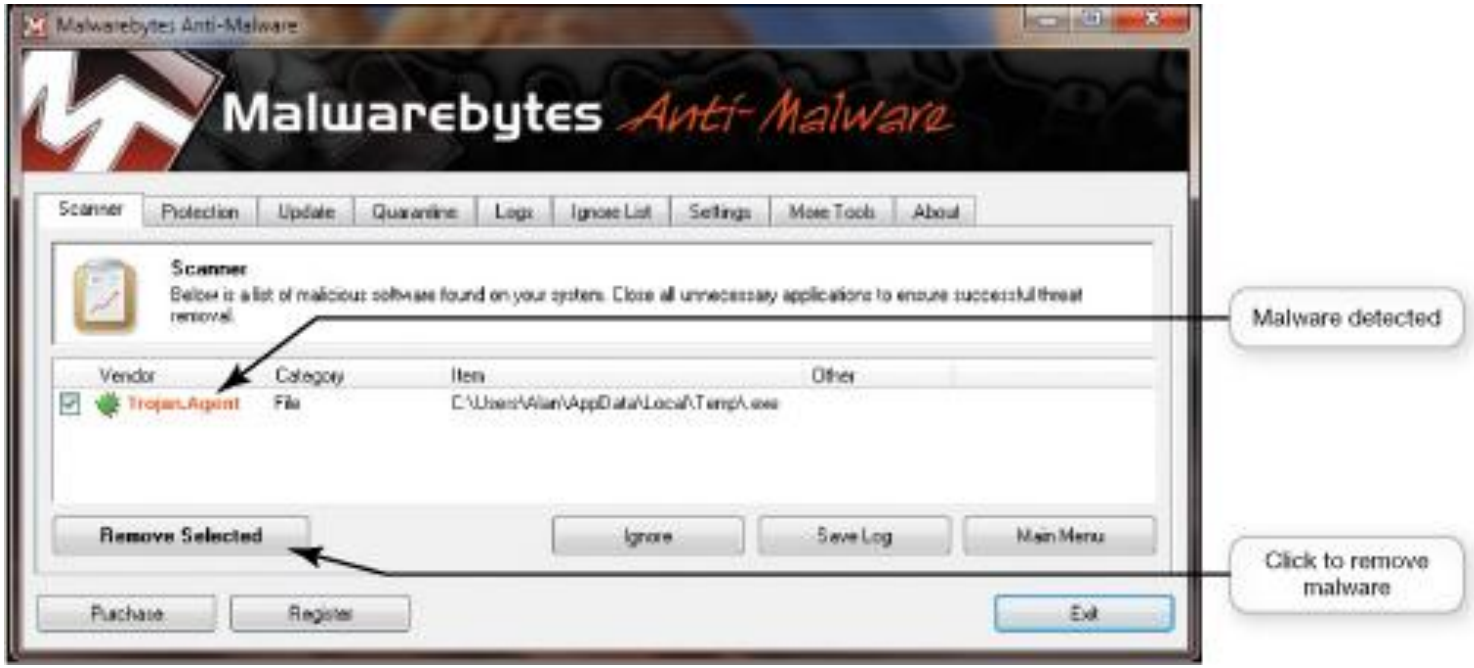
Spyware

- Spyware: Neželjeni program koji se obično dowload-uje sa drugim softverom koji instalirate sa Interneta i izvršava se u pozadini:
  - Prenosi informacije o korisniku
  - Koristi *špijunske cookies*
  - *Keystroke logger*: Prati kucanje po tastaturi za krađu loziniki, naziva korisnika ili informacija kreditnih kartica.

Anti-spyware

- *Anti-spyware* softver: otkriva neželjene programe i omogućava njihovo brisanje.
- Preporuka instalirati 1 ili dva samostalna anti-spyware programa.
- Danas većina *Internet security suite* obuhvata i antispyware programe.

Anti malware



Managing Online Annoyances
Spam

- SPAM: Neželjeni ili “đubre” e-mail
- SPIM: Neželjen instant poruke
- REŠENJE: kreirati e-mail adresu koju ćete koristiti samo za popunjavanje formi ili poručivanje stvari na Internetu.

Spam

- Iako je većina ljudi svesna postojanja spama, prema istraživanju MAAWG **polovina** e-mail korisnika u Severnoj Americi i Evropi je otvorila spam, od kojih su neki kreirani za otrkrivanje osetljivih informacija.
- 46% ljudi koji su otvorili spam su to uradili namerno.

- Messaging Anti-Abuse Working Group (MAAWG)

Spam

- Spam filter: Opcija koju možete da selektujete u vašem e-mail nalogu koja postavlja spam u specijalni folder.
- SPAMfighter
- Spam fileter i softver za filtriranje može da uhvatiti oko 95% spama proverom dolaznog maila preko zaglavlja *subject-a,* adrese pošiljaoca postojećeg spama i dr..spam paterni (“for free”, “over 21”).
- Spam filteri nisu idealni, i može se desiti ponekad i greška.

Spam

- Drugi načini da se izbegne spam
  - Čitati politiku privatnosti web sajta i ne davati dozvolu sajtu da prođe do vaše e-mail adrese.
  - **Ne odgovarati na spam.** Odgovaranjem vi samo potvrđujete da je vaša email adresa aktivna i umesto stopiranja spama, možda ćete dobijati još više.
  - *Postoje i dodatni servisi koji pregledaju vaš e-mail, i prosleđuju samo one poruke koje su u redu (npr. VersaForward, Sneakmail.com)*

FB spamer kažnjen sa 873.000.000$

- Adam Guerbuez za poslao **2 meseca** više od **4 mil. spam poruka** korisnicima FB (*reklamirao marihuanu i lekove za poboljšanje seksualne funkcije*).
- FB u tužbi naveo da je Adam phishing napadima **krao lozinke** za Facebook naloge i koristio **bot mrežu** hakovanih kompjutera za neovlašćeni pristup korisničkim nalozima.
- Sudija Višeg suda u Kvebeku, obrazložio je svoju presudu rečima: “Facebook nikad nije bio napadnut sa toliko mnogo **spam** poruka a metod koji je korišćen bio je posebno efikasan jer se činilo da spam poruke korisnicima šalju prijatelji.”
- Adam G. nema nameru da plati (namerava da progalasi bankroti); na svom blogu objavljuje svoju verziju događaja, hvali se životom na “visokoj nozi” i planira da unovči priču, objavljivanjem knjige ili snimanjem filma.
- U FB veruju da će uspeti da naplate kaznu koju je izrekao sud.

Cookies (kolačići)

- Cookeis (kolačići): mali tekstualni fajlovi koje neki web sajtovi automatski čuvaju na vašem hard disku.
- Kada se prijavite na website koji koristi cookies, cookies dodeljuje ID broj vašem računaru. Jedinstven ID –namera da se efikasnije vrati na web sajt. Sledeći put kad se prijavite na sajt, sajt će označiti vašu posetu i čuvati podatke u bazi.
  - Obezbeđuje websajt sa informacijama o vašim navikama pregledanja: šta ste pregledali, kada i koliko je trajalo.
  - Praćenjem takvih informacija, cookies omogućavaju kompanijama da identifikuju različite preference korisnika.

Cookies

- *Cookies* ne traže personalne informacije kao što su lozinke i ili fin. podaci, već samo sakupljaju personalne informacije koje se daju prilikom popunjavanja formi.
- Neki sajtovi prodaju ovako skupljene informacije web oglašivčima koji prave velike baze korisnikovih preferenci i običaja, sakupljajući lične i poslovne informacije kao što je broj telefona, kreditni izveštaj i sl. Cookies ne predstavljaju nikakvu pretnju po bezbednost (u njima se ne skriva maliciozni softver) oni mogu da naruše vašu privatnost.

ČUVANJE PODATAKA

“Sigurni podaci”

- Ljudi često imaju previše poverenja ili nehajni su kada se radi o njihovim privatnim informacijama ili digitalnim podacima.
- Neophodno je zaštiti podatke od oštećenja: slučajnog ili namernog.

Čuvanje vaših ličnih informacija

- Osnovno pravilo: Odavanje što manje informacija, pogotovo ako su informacija dostupne svima
- Ne bi trebalo ostavljati javno dostupno sledeće informacije matični broj, br. telefona, datum rođenja adresa.
- Sajtovi za socijalno umrežavanje imaju dodatna podešavanja privatnost; inicijalno svima je dostupno.
- Za većinu podešavanja postaviti Friends ili Only Me.

Rezervna kopija (back up) podataka

- Podaci na računaru se suočavaju sa tri osnovne pretnje:
  - Neautorizovan pristup
  - Uništavanje
  - Izmena
- Haker može da pristupi računaru i ukrade i izmeni podatke. Ipak, verovatnije je da se izgube/oštete podaci nenamerno (oštećenje hard diska, virus uništava fajl, uništenje računara…)
- *Back-up* su kopije fajlova koje mogu se koriste ako se original ošteti ili uništi.

Rezervna kopija podataka

- Tipovi rezervnih kopija
  - Inkrementalni (back-up samo izmenjenog)
  - Potpuni
- Gde sačuvati back-up fajlova
  - Online u “oblaku”
  - Eksternom hard disku
  - Mrežnim uređajima za skladištenje ili serverima.

Rezervna kopija podataka

- Dve glavne opcije za pravljenje rezerve kopije fajlova (back up):
  - Inkrementalni back up (parcijalni backup): Pravljenje rezerevne kopije samo fajlove koji su izmenjeni ili kreirani od prethnog back up-a.
    - Efikasniji
  - Image back up (Back up sistema): Za ceo sistem, aplikacije i podatke se kreira rezervna kopija. Ideja da postoji egzaktna kopija hard diska i moguća je u potpunosti da se konfiguriše kao pre kraha.

Rezervna kopija podataka

- Backups trebali da budu sačuvani na bar dva sigurna mesta, ne pored kompjutera.
- Postoje tri izbora:
  - Online (in the cloud; free npr. MS SkyDrive, za veće količine Carbonite ili iBackup)
  - Eksterni hard diskovi (lokacija?, u kombinaciji sa još nečim)
  - Network-attached storage (NAS) uređaji i home servers: NAS uređaji su veliki hard drajvovi koji su povezani na mrežu računara umesto samo a 1 računar, i mogu se koristiti da backup-uju više računara simultano.

Poređenje uobičajenih lokacija za rezerevne kopije

Lokacija	Prednosti	Mane
Online (u oblaku)	•Fajlovi se čuvaju na sigurnoj, udaljenoj lokaciji •Fajlu se može pristupiti od bilo gde preko browsera	•Većina besplatnih sajtova ne obezbeđuje dovoljno porstora za image backup •SIgurnost?
Eksterni hard diskovi	•Jeftini •Brz backup sa USB3.0 uređajima povezanim direktno na računar	•Mogu se uništiti u jednom događaju •Mogu se ukrasti •Teško backup-ovanje više računara sa jednim uređajem
NAS (Netowork Attached Storage) Home Servers	•Prave rezervne kopije lakše za većinu komjuterskih uređaja.	•Skuplji nego samostalni eksterni hard drajv •Može se uništiti u poplavi/požari zajedno sa računarom •Može se ukrasti.

SOCIJALNI INŽENJER

Socijalni inženjering

- Socijalni inženjer: bilo koja tehnika koja koristi socijalne veštine da generiše ljudsku interakciju koja izmamljuje individue da otkrije osetjive informacije
  - Često ne uključuje računare ili interakciju licem-u-lice.
  - Mnogi namame žrtve, kreirajući scenarijo koji zvuči dovoljno legitiman da će neko poverovati, npr phishing.

Socijalni inženjering

- Primer: Dobijete telefonski poziv, gde vam kažu da su iz vaše banke i da neko pokušava da koristi vaš nalog bez autorizacije.
- Potrebno da potvrdite nekoliko ličnih podataka, kao što je datum rođenja, matični broj, broj računa iz banke, i bilo koju drugu informaciju koju može da izvuče iz vas.
- Informaciju koju dobije na taj način on koristi da isprazni vaš račun ili izvrši neku drugu prevaru.

Phishing i Pharming

- **Fišing** (eng. phishing): “Privlači” Internet korisnike da odaju personalne informacije kao što su brojevi kreditnih kartica, matični broj, ili druge osetljive informacije.
  - Prevare e-mailom
- Farming (engl. Pharming): maliciozni kod je podmetnut na tvom računaru, ili preko virusa ili posetom malicioznih websajtova.
  - Podmukliji od fišinga
  - Menja sposobnost browsera da pronađe web adrese.

Phishing i pharming

- Preporuke za izbegavanje fišinga i farminga:
  - Nikada ne odgovarajte direktno na e-mailove u kojima se traže vaše lične informacije.
  - Ne “klikćite” na linkove u e-mailovima da biste otišli na web sajt.
  - Ne ostavljajte lične informacije preko Interneta sem ukoliko je sajt siguran.
  - Koristiti filtere za fišing browsera.
  - Koristiti Interent sercurity softver koji je redovno ažuriran.

Phishing i pharming

- *Internet security* paketi mogu da detektuju i spreče PHARMING napade:
  - McAfee ili Norton

Phishing

- Phishing opasna Internet prevara
- Koriste se podaci dostupni iz socijalnih medija i omogućava zlonamernoj osobi da napravi profil žrtve da bi ga bolje ubedila da je prevara realna.

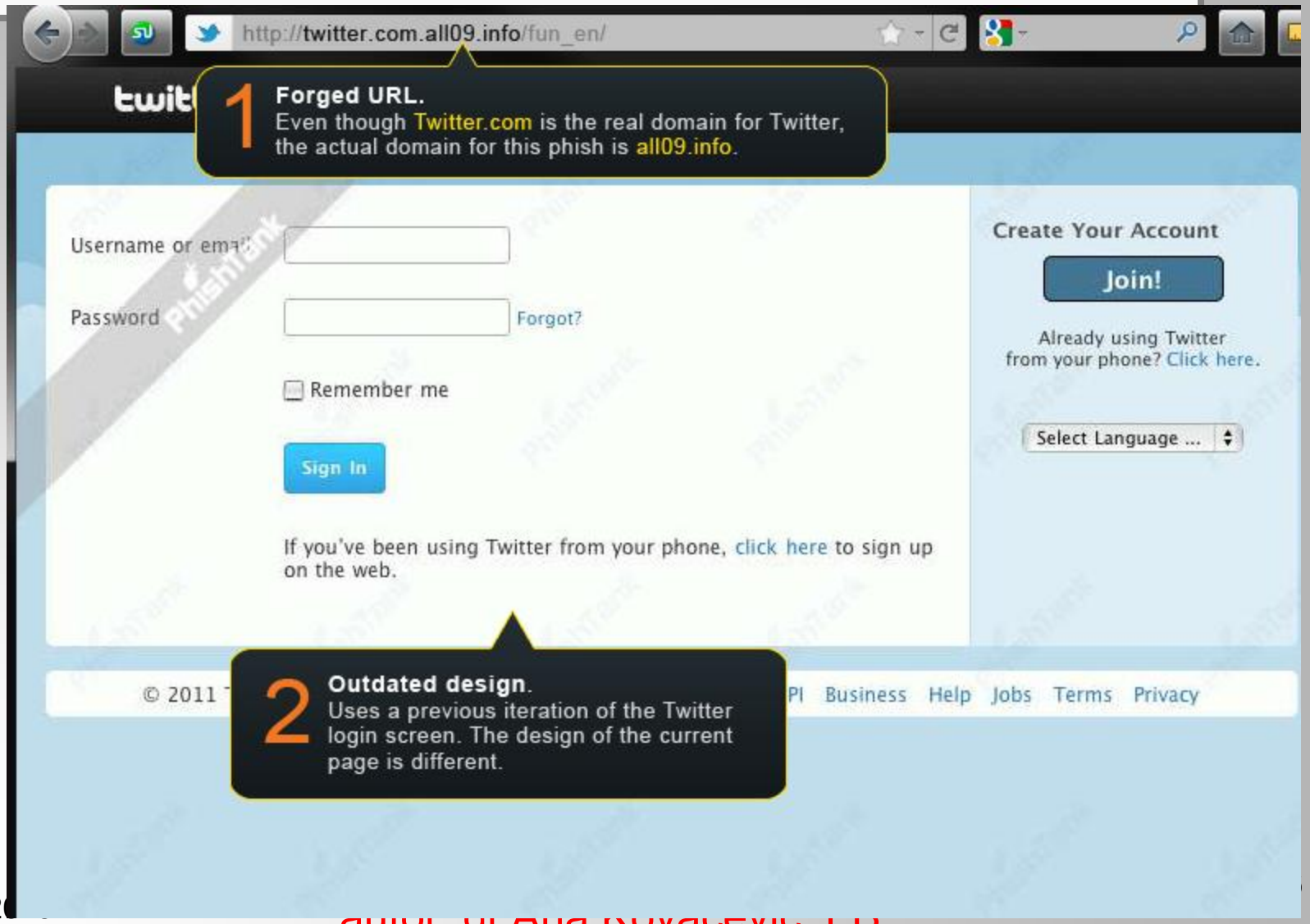
Phishing-primer

1. Žrtva prima naizgled poslovni mail koji je stigao od “sigurnog” izvora, kao onlinebanking sajta ili…
2. U emalu stoji da je neophodno da se ažurira nalog odmah ili će biti suspendovan na nekoliko dana.
3. Email sadrži URL (link) i upućuje korisnika da klikne na link i ažurira informacije. Tekst linka kao za očekivani sajt, no link je veza do napadačevog sajta (koji je napravljen da izgleda kako korisnik očekuje da vidi).
4. Na lažnom sajtu, korisnik unosi ID/password
5. Sajt javlja uobičajenu poruku npr. “We’re sorry- we’re unable to process your transaction at the time”
6. Žrtvini podaci su kod napadača koji može njima da se koristi.

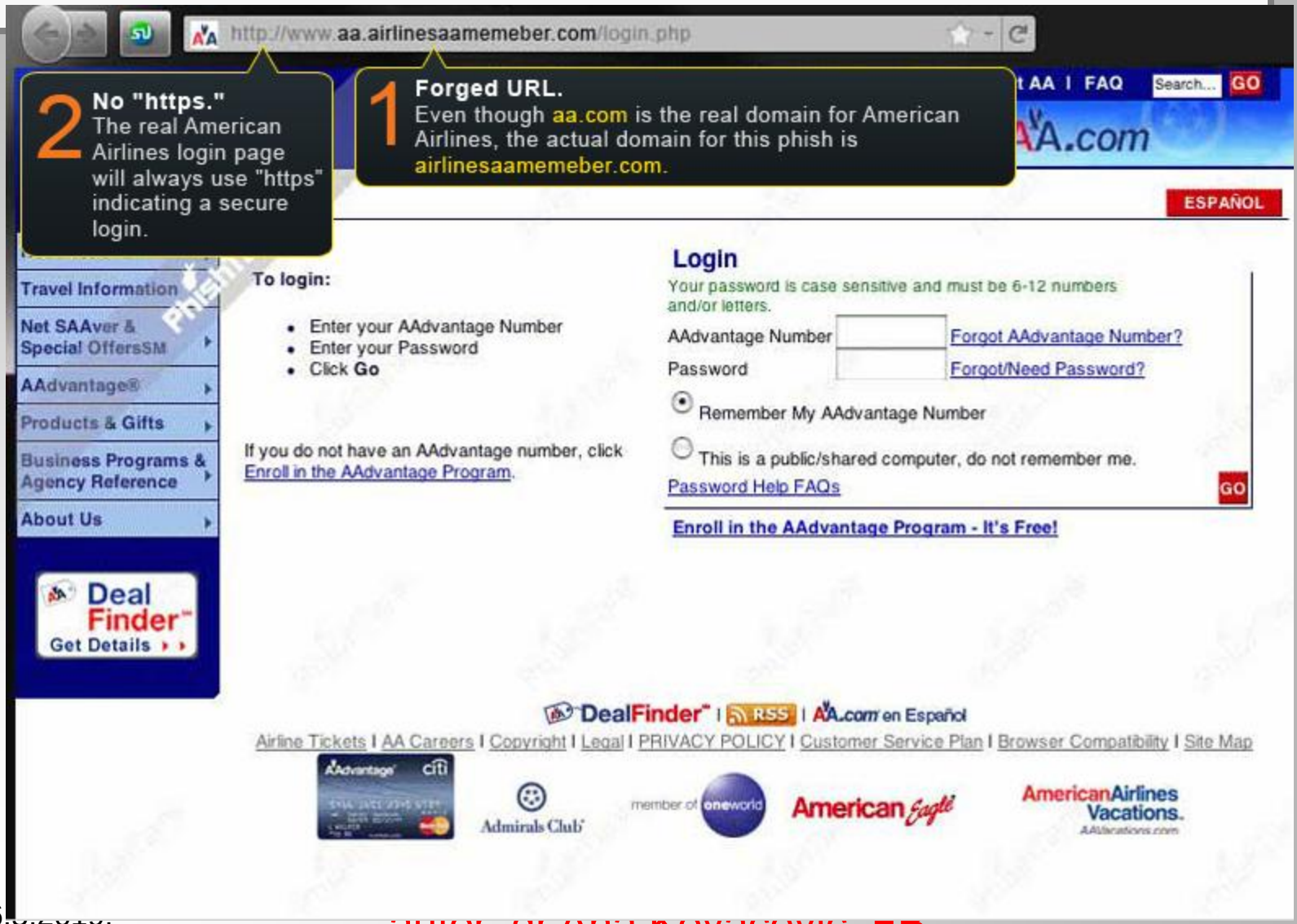
Zaštita od phishinga

- “Osvešćavanjem” i edukacijom
- Uočiti znakove prevare: phishing mail umesto imena koristi *User* ili na osnovu email adrese;
- Nikada ne kliknuti na linkove u netraženim finansijskim mailovima. Iako link izgleda regularan on vodi do sajta napadača.
- Proveriti prijavljivanje na regularan sajt.
- Proveriti sa vašim provajderom (organizacijom, bankom…) vezano sa phishing prevare za koje znaju.

Primer: Phishing



Primer: Phishing



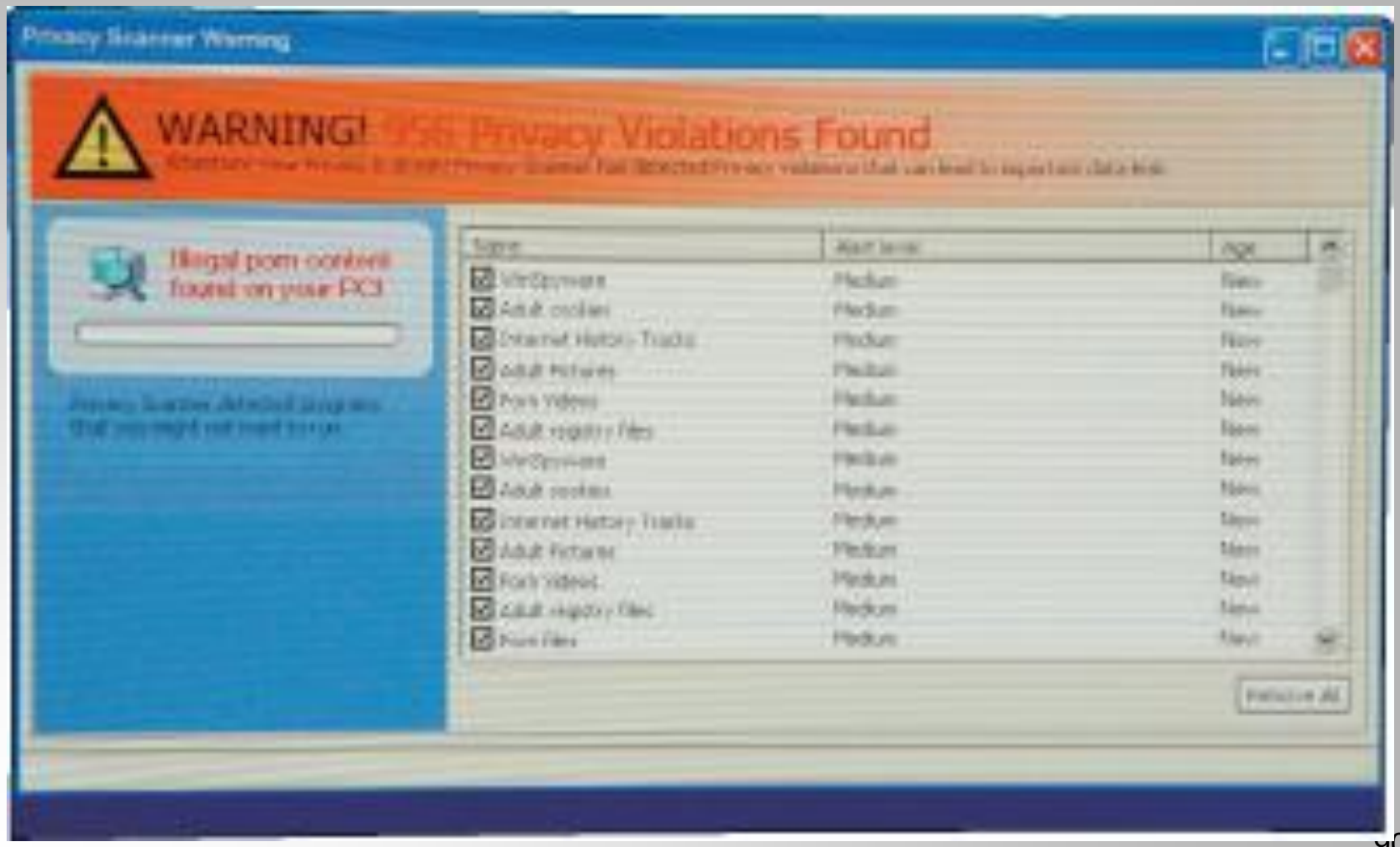
Scareware

- Scareware: Zlonamerni program koji je dowload-ovan na vaš računar i pokušava da vas ubedi da vam je računar zaražen virusom ili drugim malverom.
  - Upućuje na websajt da se kupi lažni čistač ili antivirusni alat sa malo ili ni malo vrednosti.
  - “Scareware” je tehnika socijalnog inženjeringa pošto koristi ljudski strah od računarskih virusa da ih ubedi za deo novca.
  - Scareware je kreiran da ga je teško ukloniti sa računara i umešan je sa operacijom legitimnog bezbednosnog softvera.

Scareware

- Scareware:
  - Obično je dowloadovan na vaš računar sa zaraženih web sajtova ili fajlova trojanaca.
  - Većina Internet security suites, AV, i anti-malware paketa sada detektuje i sprečava instalaciju scareware-a.

Scareware: Primer



Literatura

- Evans, Martin, Poatsy „Technology in action“ 10th edition, 2014