RƏQƏMSAL TƏHLÜKƏSİZLİK

Bələdçi

İyun 2016

RƏQƏMSAL TƏHLÜKƏSİZLİK

Bələdçi

İyun 2016

Mündəricat

İnternet təhlükəsizliyi niyə vacibdir?

İnternet təhlükəsizliyini günədlik həyatımızda tez və asanlıqla təmin etmək elə də asan deyil. Rəgəmsal təhlükəsizlik kompüter anlayışından xeyli kənara çıxır. Bu barədə düşünərkən ilk növbədə hansı məlumatları qorumaq istədiyimizi bilməliyik. O biri tərəfdən isə hansı növ təhlükələrin qarşımıza çıxacağının və bu təhlükələri neytrallaşdırma vasitələri barədə tam təsəvvürümüz olmalıdır. Rəqəmsal təhlükəsizliyin əhatəsi bizim fəaliyyətimizdən və yaşadığımız yerdən asılı olaraq dəyişə bilər. Siz biznesdə, dövlət sektorunda və ya vətəndaş cəmiyyətində çalışa bilərsiz. Bu halda özəl məlumatların xüsusiyyəti fərqli ola bilər. İstər fəaliyyət sahəsində, istərsə də şəxsi həyata aid özəl məlumatlar ola bilər. Burada bank kartlarının şifrələrindən tutmuş biznes ideyalarına kimi bir çox məlumatlardan söhbət gedir. Amma, hər bir halda problemin miqyasını anlamaq və həll yollarını müəyyən etmək üçün təhlükəni modelləşdirmək gərəkdir.

Bu halda beş önəmli sual yaranır

1. Məhz hansı məlumatı qorumaq istəyirsiniz?
2. Məlumatı kimlərdən qorumaq istəyirsinz?
3. Sizin onu qorumaq imkanınız hansı səviyyədədir?
4. Məlumatlarınıza nəzarəti itirdiyiniz halda nəticəsi nə ola bilər?
5. Nəticələrin qarşısını almaq üçün hansı resursları sərf etməyə hazırsınız?

Ümumi təsəvvürlərə görə bütün rəqəmsal cihazlar təhlükəsizdir. Nəzəri cəhətdən rəqəmsal cihazlar başqa şəxs və ya şəxslər tərəfindən nəzarətə götürülməkdən və izlənməkdən qorunmalıdır. Amma çox təəssüf ki, bu belə deyil. Viruslar, hakerlər, şəxsi məlumatların ələ keçirilməsi üçün casus proqramlar, izləmələr və s. bizi ehtiyatlı olmağa vadar edir. Rəqəmsal dünyada biz təhlükəsizliyi təmin etmək üçün müəyyən vaxtlarda əlavə alətlərdən faydalanmalıyıq. Bu bələdçidə biz bəzi üsullar təklif edirik, bunlar rəqəmsal cihacları viruslardan qorumaqdan tutmuş özəl məlumatların şifrələnməsinədək çoxsaylı alətləri əhatə edir.

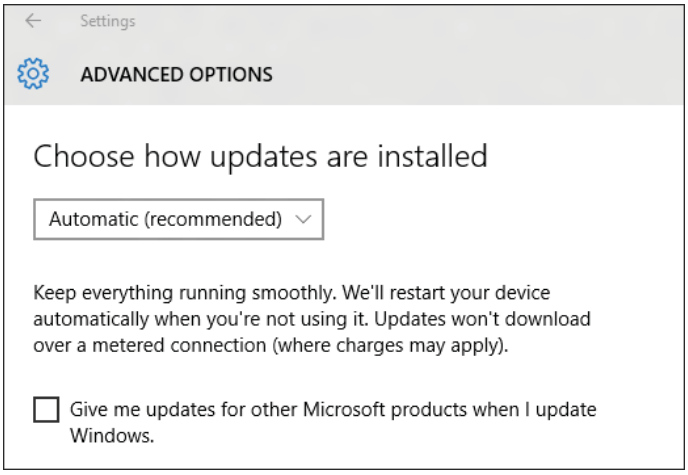
1. Kompüterdə profilaktika və təhlükəsizlik

- **Windowsun yenilənməsi** - bu funksiya Microsoft tərəfindən təqdim olunur, hansi ki, Microsoft Windows əməliyyat sistemini təmin edir. Yenilənmə nəinki əməliyyat sistemini, elecədə Microsoftun digər proqramlarını da yeniləyir (Internet Explorer, Microsoft Office, Microsoft Security Essentials və Microsoft Expression Studio).

Bununla biz kompüterimizdə yeni funksiyalar əldə edirik, əlavə təhlükəsizliyə və sürətə nail oluruq.

Windowsun avtomatik yenilənmə növünü seçin

Start düyməsinə keçin - Parametrlər bölməsini seçin - Yenilənmə və təhlükəsizlik- Windows yenilənmə mərkəzi- əlavə parametirlər.



Antivirus

Kompüter virusları həyatımızı çətinləşdirir. Onlar faylları və disklərdəki bölmələri, məlumatları məhv edir və cihazların yavaş işləməsinə səbəb olur. Hiyləgərcə ünvan kitabından istifadə edərək, öz spamlarını bizim dostlarımıza və iş yoladşlarımıza göndərillər. Bunların baş verməməsi üçün çoxsaylı antivirus proqramları mövcuddur.

Mövcud olan proqramlardan biri:

Ödənişsiz Avast programıdır.

AVAST

(https://www.avast.com)

Düşünmək lazım deyil ki, antiviruslar bahalı olmalıdır. Pulsuz olan Avast – kompüterin təhlükəsiliyi üçün güclü alətdir. Digər antiviruslar kimi Avast da kompüteri skan etmək, virusları axtarıb və silmək, sistemi virusa yoluxmaqdan qorumaq və internetdən avtomatik olaraq antivirus bazasını yeniləmək imkanlarına malikdir.

Antivirus istifadəçiləri mütləq iki qeydi yadda saxlamalıdır.

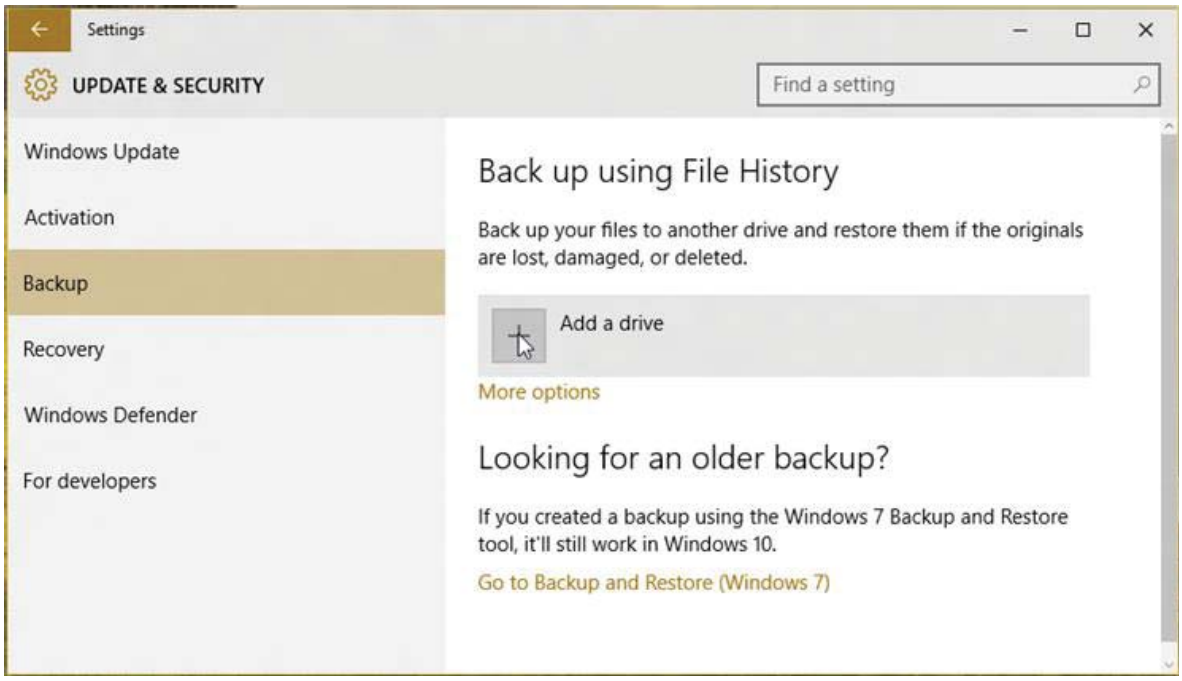
1. Hiyləgərlər tərəfindən daimi yeni viruslar yaradılır. Buna görə antivirus bazasını internet üzərindən dami yeniləmək və buna əngəl yaratmamaq lazımdır.
2. Eyni zamanda iki və ya daha çox antivirus çalışdırmaq konfliktə və əməliyat sisteminin yavaş işləməsinə səbəb ola bilər. Oddur ki, antivirusu yükləməmişdən öncə sistemdə başqa antivirusun olmadığına əmin olmaq gərəkdir.

Faylların nüsxələrinin yaradılması (Backup)

Faylların nüsxələrinin yaradılması informasiyanın (faylların, proqramların və parametirlərin) zədələndiyi anda qısa bir müddətə bərpa etmək imkanı yaradır.

Faylların nüsxələrinin yaradılması Windows 10-da

Start düyməsinə keçin - Parametirlər bölməsini seçin - Yenilənmə və təhlükəsizlik- Faylların nüsxələrinin yaradılması- Diski əlavə etmək və xarici disk və ya Back up üçün şəbəkə yerini seçin.



Faylların nüsxələrini onlayn “cloud drive”dan (bulud yaddaşı) istifadə edərək backup etmək mümkündur. Bununla siz öz məlumatlarınızı istənilən yerdə əldə etmək imkanı qazanırsız. Bulud yaddaşından istfadə etmək üçün bir neçə sistem mövcuddur.

Dropbox - www.dropbox.com

Google Drive - www.google.com/drive

Mega - www.mega.nz

OneDrive - www.onedrive.live.com

Qeyd: Bulud yaddaşında qeydiyatdan keçdikdən sonra 2 addımlı doğrulama sistemini goşmaq arzu olunandır.

■ Disklərin şifrələnməsi

Disklərin şifrələnməsi – informasiyanin şifrələnmə texnologiyası kənar müdaxilə nəticəsində diskdəki məlumatların oxunmasının və deşifrə edilməsinin qarşısını alır. Şifrələşdirmək üçün xüsusi proqramlardan və yaxud cihazdan istifadə etmək mümkündür ki, bu da yaddaşın hər bir bölümünü şifrələyir.

Disklərin şifrələnməsi üçün bir sıra proqram təminatı mövcuddur. Bunlardan FDE (full disk encryption) texnologiyasına malik olan proqramlar daha populyardır: BitLocker və Veracrypt

BitLocker - məlumatın diskdə (disklərdə, SD kartda və USB yaddaş kartında) tam şifrələnmə yolu ilə qorunmasını təmin edir. Beləliklə hiyləgərlər sizin sistem fayllarına və fiziki olaraq məlumatların digər kompüterdə oxunulmasının qarşısını alır.

BitLockeri aktivləşdirmə

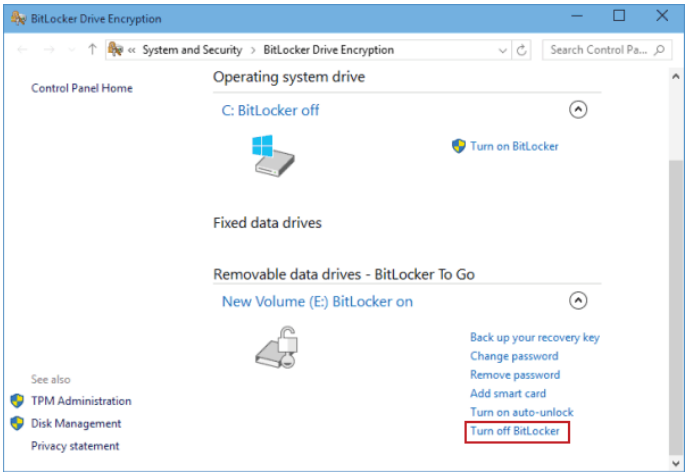
ƏLAVƏ

Disklərin şifrələnməsi BitLocker yalnız Windows 8.1 profesional və Windows 8.1 koorporativdən yuxarı olan əməliyyat sistemlərində mövcuddur.

XƏBƏRDARLIQ!

BitLocker aktivləşdirmə zamanı bərpa açarını yaratmağı unutmayın. Əks halda siz öz məlumatlarınıza girişi əbədi itirə bilərsiniz.

1. BitLocker bölməsini açın. Bunun üçün Windows-un axtarış sisteminə **BitLocker** sözünü daxil edin. BitLocker səhifəsi açıldıqdan sonra parametrlər bölməsindən **Diskin BitLockerlə Şifrələnməsinə** (BitLocker Drive Encryption) keçid alın.
2. BitLockeri aktivləşdirmək bölməsinə keçin. Sizdən administrator kimi daxil olmaq və yaxud seçiminizin təsdiqlənməsi tələb oluna bilər.



3. Təlimatları izləyin

2. İnternet təhlükəsizliyi

Hesabların təhlükəsizliyi

Rəqəmsal dövrün aktual problemlərindən biri də hesabların oğurlanmasıdı. Hiyləgərlər hesabların (email, sosial şəbəkələr, bank hesablar və s.) ələ keçirmək üçün bir çox üsullardan istifadə edirlər. Bu hücumların əsası **sosial mühəndislik** (Social engineering (security)) əsasında qurulub.

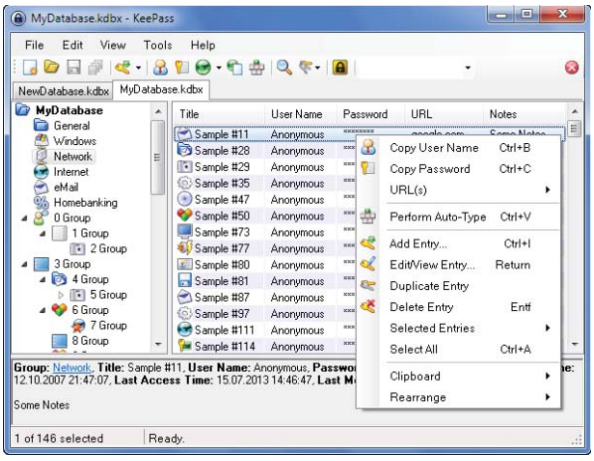
Hesabların təhlükəsizliyi üçün bir sıra mühüm tədbirlər görülməlidir:

Parol siyasəti

E-poçt və sosial şəbəkə hesablarının oğurlanmasının əsas səbəblərindən biri də çox sadə parollardan istifadə edilməsidir. Araşdırmalar göstərir ki, istifadəçilər öz şifrələrini unutmamaları üçün, ya 123456 kimi olduqca sadə şifrələrdən, yaxud telefon nömrələrindən və ya təvəllüdlərindən istifadə edirlər ki, bu da onları yaxından tanıya bilən adamlara asanlıqla onların hesablarını ələ keçirməyə imkan yaradır. Bu səbəbdən mürəkkəb parolların yaradılması üçün aşağıdakılar tövsiyyə olunur:

1. Parollar bütöv bir sözü ifadə etməməlidir.
2. Ən azı 8 simvoldan ibarət olmalıdır.
3. Böyük və kiçik hərflərdən təşkil olunmalıdır.
4. Rəqəmlərdən istifadə olunmalıdır.
5. Simvollardan da istifadə olunmalıdır (~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /)

KeePass



KeePass **(**www.keepass.info**)** – müxtəlif sayt və xidmətlər üçün hesab parollarının təhlükəsiz saxlama proqramıdır. Bu proqramın daxilində hesab üçün hücumlara davamlı parol yaradılaraq yadda saxlayırlar. Siz yalnız əsas parolu bilməklə digər parollarınızı deşifrə edərək əldə edə bilərsiniz. Proqramı siz USB fleşdə quraşdırmaqla proqramı digər kompüterlərdə də istfadə edə bilərsiniz.

Gmail / Facebook / Twitter / Skype

Hesabların təhlükəsiz olduğuna əmin olmaq üçün aşağıda sadalananlara əməl etmək məsləhət görülür.

1. Hesabların təhlükəsizliyini yoxlamaq. Hesabın tənzimləmələr bölməsinə keçərək, bunu yoxlamaq mümkündür.
2. Hesablara girişi bərpa etmək üçün istifadə olunan məlumatı daim yeniləmək. Hesabın bərpa parametirlərinin düzgün qeyd olunduğuna əmin olmaq.
3. İki addımlı doğrulama giriş sistemini aktivləşdirin. Bu hesabın əlavə qorunmasını təmin edəcək. Giriş zamanı sizdə şifrə ilə yanaşı telefon nömrəsinə gələn kodu daxil etmək tələb ediləcək.
4. Bir şifrəni bir neçə hesabda istifadə etməmək! Bu halda bir hesab oğurlanarkən o biri hesabların da oğurlanmasına imkan yaranır.

İki Addımlı Doğrulamanın aktivləşdirilməsi:

1. **Gmail** – Mənim hesabım - Təhlükəsiz giriş- Google hesabına giriş - İki Addımlı doğrulama (2 step verification)
2. Təlimatları izləyin

Facebookda iki addımlı doğrulamanın aktivləşdirilməsi:

1. Tənzimləmələr- Təhlükəsizlik – Girişin təsdiqi
2. Təlimatları izləyin

Twitter-də iki addımlı doğrulamanı aktivləşdirilməsi

1. Tənzimləmələr- Təhlükəsizlik və Məxfilik - Girişi təstig etmək
2. Təlimatları izləyin

İnternet kanallarının qorunması – https

HTTPS (Hypertext Transport Protocol Secure) – Sayt və istifadəçinin cihazı arasında rabitə təhlükəsizliyini və məxfiliyini təmin edən protokoldur. M əsələn, bir istifadəçi yeniliklərə abunə və ya bir məhsul almaq üçün, sizin saytda bir formaya məlumat daxil etdikdə, HTTPS istifadəçinin və saytın arasında şəxsi məlumatları qoruyur. Hər bir istifadəçi bu məlumatların

hiyləgərlərin əlinə düşmədiyinə ümüd edir. Məlumatları qorumaq üçün, HTTPS protokolundan istifadə edin.

Hər yerdə https

Https protokolundan istifadə edən saytlarda, məlumatların bütövlüyünü TLS (Transport Layer Security) təmin edir və üç prioritet bölümü istifadə edir.

1. Şifrələnərək məlumatları ötürür və kənar şəxslərin ələ keçirilməsinin qarşısını alır. Buna görə də təcavüzkarlar sayt istifadəçilərin bölüşdükləri məlumatları və onların səhifələrdəki addımlarını izləyə bilmirlər.
2. Doğrulama. Bu istifadəçilərin onlar lazımı sayta daxil olmasını təmin edir və orda hücumlardan qoruyur.

VPN

VPN (Virtual Private Network) - məlumatları virtual tunnel vasitəsi ilə şifrələyərək ötürən əlaqə vasitəsidir. VPN-lər iki əsas işi həyata keçirirlər. Birincisi, iki nöqtə arasında virtual tunnelin yaradılması və ikincisi, həmin tunel daxilində gedən informasiyanın şifrələnməsidir.

VPN üçün istifadə olunan proqramlardan biri də s**ecuritykiss**di **(www.securitykiss.com)**

Securitykiss Tunnel – virtual özəl şəbəkədir, OpenVPN və L2TP əsasında fəaliyyət göstərir. Securitykiss proqramının ödənişsiz versyası sizə günlük 300 Mb trafik və dörd ölkədə yerləşən serverlərdən istifadə imkanı verir.

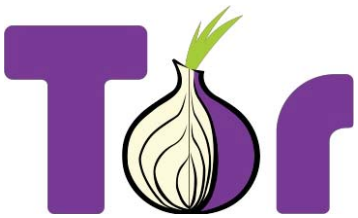
Browser

İntrernet saytlarının oxunması üçün biz brauzerdən istifadə edirik. Hazırda ən çox istifadə olunan brauzer (browser) Internet Explorer, Opera, Safari, Mozilla, Google Chrome-dur. Statistikaya görə istifadəçilər daha çox Googel Chrome və Firefoxa üstünlük verir.

Təhlükəsiz şəkildə saytlara daxil olmaq üçün Chrome və Firefox brauzerlərinin internet-mağazalarından (web-store) aşaqdakı əlavələri yükləyə bilərsiniz:

1. **BrowSEC** və ya **ZinMate** – virtual özəl şəbəkə
2. **Adblock Plus** – Saytlara reklamsız bax
3. **HTTPS Everywhere** – saytlara təhlükəsiz daxil ol

Tor Browser



Tor Browser (www.torproject.org) - internetdə senzuradan yayınma alətlərindən biridir. O, istifadəçilərə onlayn addımlarının məxfiliyini qorumaq üçün yaradılıb. Bu alət internet istifadəçilərinin məlumatlarının xüsusi saytlar və onlayn casuslar tərəfindən ələ keçirilməsini çətinləşdirir. Tor istifadəçilərə imkan yaradır ki, məxfiliyi təmin etməklə yanaşı internetə daxil olduqları ərazidə baxılmasına qadağa qoyulmuş məlumatlara çıxış əldə etsinlər. Tor istifadəçilərin internet bağlantısını və məlumatlarını bir sistem vasitəsilə yönəldir, bu sistem təsadüfi seçilmiş relelərdən ibarətdir. Bu, təmin edir ki, istifadəçilərin məlumatları istəmədikləri insanlar tərəfindən əldə edilməsi mümkün olmasın.

Tor Browser-i siz həmçinin Android və IOS sistemli telefonlara da internet mağazadan Orbot və Orweb yazmaqla yükləyə bilərsiniz.

3. Təhlükəsiz ünsiyyət

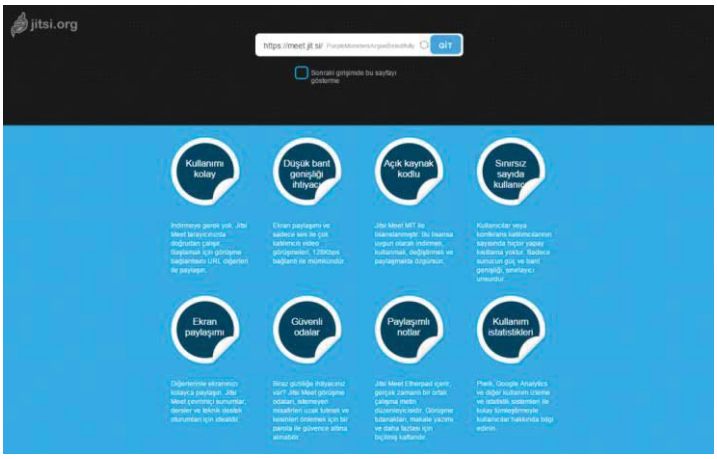
Telefonunuzla zeng etdiyimiz, SMS yazdığımız, elektron məktub aldığımız an və yaxud Facebook, Google Hangouts mesaj oxudugumuz zaman kənar insanlar bizim yazdıqlarımızı, kiminlə danışdığımızı və harda olduğumuzu izləyə bilərlər. Bu şəxsi məlumatlar nəinki proqram tərtibatçısı, həmçinin internet provayderləri, kəşfiyyat xidmətləri əldə edə bilər.

Lakin siz məlumatlarınızın təhlükəsizliyi ilə bağlı zəruri tədbirlər tədbiq etməklə qizli-anonim onlayn mesajlar göndərə bilərsiniz. Şifrələnilmiş və anonim usulla ünsiyyət yaratmaq üçün bir sira proqramlar mövcuddur.

Jitsi

Jitsi (www.jitsi.org) - internet üzərindən ani mesajlaşma, səsli və göruntünü dəstəkləyən pulsuz və Open Source proqramdır. Jitsi bir sıra m əhşur protokolları, ani mesaj və telefoniyanı dəstəkliyir, öz əliklə SIP (Session Initiated Protocol), Jabber/XMPP(Facebook və Google Talk-da istfadə olunur), AIM,ICQ,MSN və Yahoo! Massenger. Proqramda OTR (Off the Record) mesajda, səs və videoda (ZRTP, SRTP) şifrələnmə növləri istifadə olunur.

Real zamanda komunikasiya (WebRTC) yaratmaq üçün meet.jit.si saytına daxil olursunuz.



Səhifədə kəsr işarəsindən sonra istənilən sözü (meet.jit.si/1234) qeyd etməklə “Go” düyməsinə basırsınız. Qeyd etdiyiniz sözü qarşı tərəfə bildirirərək, ünsiyətə keçirsiniz.

WebRTC texnologiyalı digər saytlarda mövcuddur: www.appear.in, www.chatb.org və s.

Şifrələnmiş Email PGP və Mailvelope

PGP (Pretty Good Privacy) - istifadəçilərin tam məxfi şəkildə elektron informasiya mübadiləsinə imkan verən, etibarlılığın yüksək dərəcəli kriptoqrafik (şifrələmə) proqramdır. PGP-də iki əlaqədar açarlardan istifadə prinsipi istfadə olunur: içtimai açar (public key) və şəxsi açar (private key). Şəxsi açara ancaq sizin çıxışınız var, öz ictimai açarınızı isə qarşı tərəf ilə bölüşürsünüz. Beləliklə qarşı tərəf sizin ictimai açarınızın vasitəsi ilə sizə şifərlənmiş məktub və yaxud fayl gondərəcək.

PGP Destkop və Mailvelope istfadəsinin əsas addımları

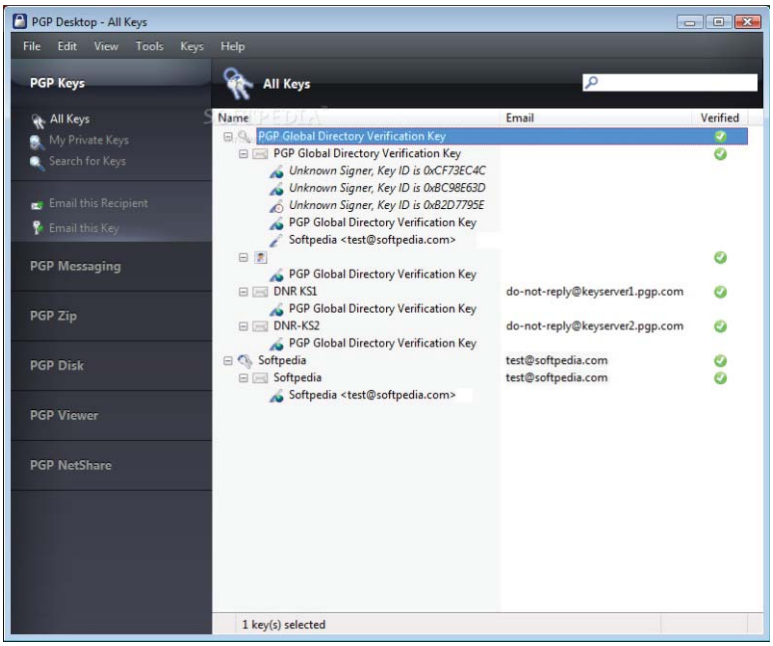
1. Təlimata uyğun olaraq proqramı yükləyin.
2. Proqramı istifadə etmədən öncə açar yaradın. Bu zaman iki cüt açar yaranacaq: şəxsi açar (tək sizə məxsus olan açar) və ictimai açar (qarşı tərəflə bölüşə biləcəyiniz açar).

3. İctimai açarı elektron poçt vasitəsi ilə qarşı tərəfə göndərin və qarşı tərəfin ictimai açarını öz siyahınıza əlavə edin.
4. Qarşı tərəf siz açarlarınızı bölüşdükdən sonra, masajı danışdıqınız tərəfin açarı vasitəsi ilə şifrəliyərək göndərə və oxuya bilərsiniz

PGP Destkop qurlaşdırılma təlimatı

Quraşdırılma zamanı əməl olunacaq tapşırıqla və mesaj başlıqlar aşağıda qeyd olunmuşdür:

1. PGP Installation program: **Next** düyməsinə basın
2. Software License agreement:nSiz lisenziya müqaviləsi ilə razısınızmı? Əgər razısınızsa, onda **Yes** basın
3. User information: İstfadəçi haqqında məlumat. Lazım olan bəndləri doldurun və **Next-i** basın
4. Setup: choose installation directory: Proqramı hara qurlaşdırılması üçün yer seçin. Dəyişiklik etmək istəmirsinizsə **Next** basın
5. Select components: **Next** düyməsinə basın.
6. Check setup information: **Next** düyməsinə basın.
7. Proqramın avtomatik açar yaratma funksiyasını işə salması üçün kompüterin yenidən başlayandan sonra düyməsinə basın "**Yes I want to run PGP keys**"
8. **Finish** düyməsinə basın və kompüterin yenidən başla sorğusuna müsbət cavab verin.



Kompüter yenidən başlayacaq və bununla da qurlaşdırma bitir.

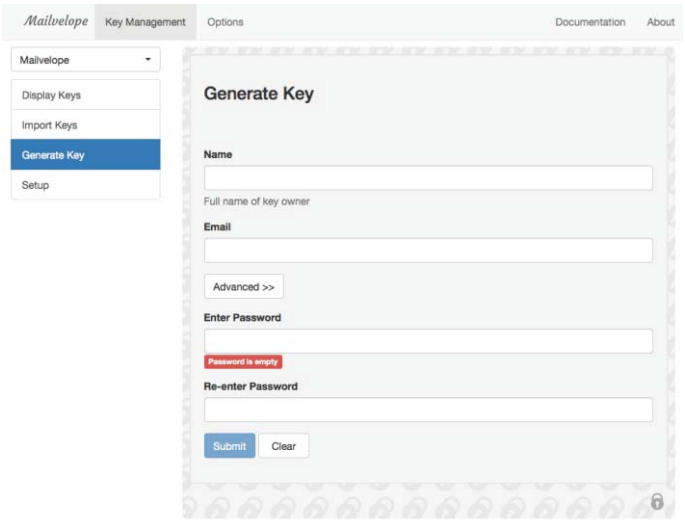
Sonra açar yatamaq lazımdır

public key – ictimai açar
private key – şəxsi açar

Mailvelope qurlaşdırılması

Mailvelope Google Chrome və Firefox üçün əlavədir. Və OpenPGP standartını istfadə edərək Gmail, Outlook, Hotmail, GMX və başqa poçt xidmətləri üçün özəl ünsiyyət imkanlarını yaradır.

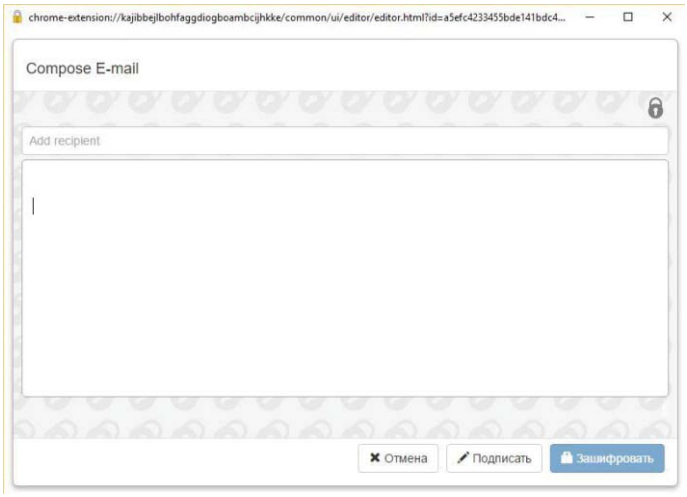
Mailvelope-yə Chrome internet mağazadan ödənişsiz qurlaşdırılır.



Yeni açarı yaradırıq

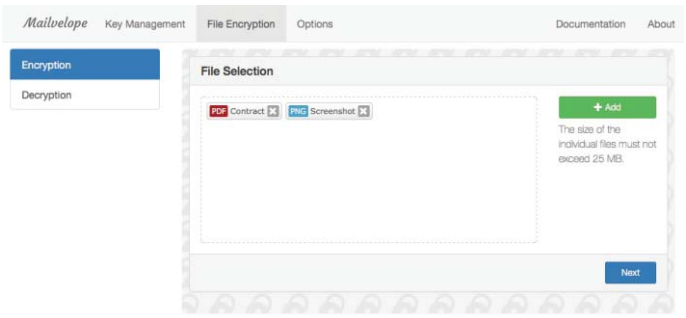
Qeyd: Daha öncə yaratdığınız açarları Mailvelope əlavə etmək olar.

Lazım olan informasiyanı daxil edib **Send** düyməsinə basın. Gmaildə sağ tərəfdə çərçivə işarəsinin üzərindən basaraq mesajın mətnini daxil edin.



Qarşı tərəfin içtimai açarını əlavə edərək mətni daxil edirsiniz və **Transfer** düyməsinə basın.

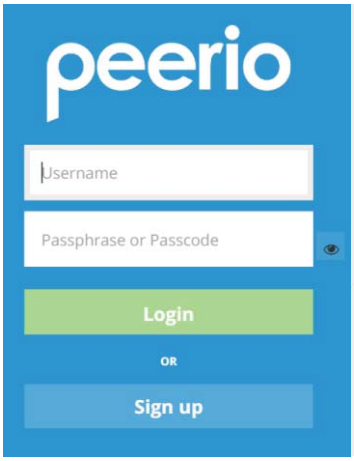
File encryption funksiyası ilə siz faylları ictimai açarlarınızla şifrələyərək öz sərt diskinizdə saxlıya və yaxud göndərə bilərsiniz. Burada şəxsi yazışmalar kimi fayıllarınızı da qarşı tərəfin ictimai açarını istifadə edərək şifrəliyərək göndərmək mümkündür.

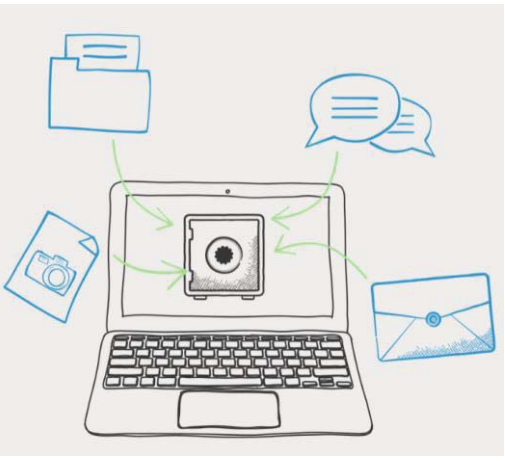


Qeyd: **Decryption** bolməsinə keçmək ilə siz faylı deşifrə edəbilərsiniz.

Peerio

Peerionun köməyi ilə sadə və təhlükəsiz yolla şəxsi yazışmalarınızı və fayllarınızı göndərə və cloud sistemində saxlaya bilərsiniz. Peerio Free sizə daxilində bütün fayllar və yazışmalar əvvəldən sona qədər şifrələnməsinə, 1 GB həcmində faylların saxlanılmasına və iki addımlı doğrulamasına imkan verir (ehtiyac olduqda həcmi artırmaq mümkündür). Proqramın Windows, Mac əməliyyat sistemləri üçün, Chrome Extension və mobil cihazlar Android və IOS üçün yükləmək olar.





4. Telefonda təhlükəsizlik

Telefonu şfrələmək (Android)

Telefonun daxili yaddaşını şifrələyərək, parol və ya PIN kod daxil edərək özəl giriş əldə etmək mümkündür. Əgər telefonda Android əməliyyat sisteminin 4.0 və ya daha təzə versiya qoşulubsa, onda cihazın şifrələnmə funksiyasından istfadə edə bilərsiniz (bütün smartfonlar dəstəkləmir). Bu zaman cihazın oğurlandığı halda şifrələnmə məlumatın qorumasına komək edir. Bununla da təcavüzkarlar sizin cihazda olan məlumatları əldə edə bilmirlər.

Qeyd: Telefonu şifrələmə zamanı smartfonda enerjinin tam dolmuş və ya enerji şəbəkəsinə qoşulması vacibdir.

Şifrələmə funksiyasını aktivləşdirmə

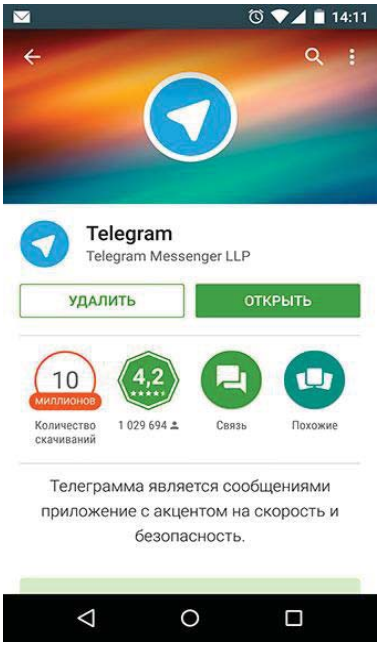
Sistemin parametri - Təhlükəsizlik - Cihazı şifrələmə bölməsinə keçid alın. Daha sonra təlimata uyğun davam edin.

Telefonu şifrələmət (IOS)

IOS4, IOS5, IOS6 və IOS 7 versiyalı əməliyyat sistemləri olan iPhone-larda siz şifrələməni “General settings” bolməsinə də “Passcode” (və ya “iTouch & Passcode”) seçərək edə bilərsiniz. IOS8 əməliyyat sistemində “Settings” bölməsində bunun üçün ayrıca “Passcode” alt bölməsi. Təlimata uyğun olaraq parol yaradın. Sizin istifadə etmədiyiniz anda telefonun killiddə qalması üçün “Require passcode” seçimini dəyişərək “Immediately” edin. Dörddən daha çox simvollu parolu qeyd etmək üçün “Simple Passcode” seçimini söndürün.

Parol tərtib etdikdən sonra tənzimləmələr bölməsinin sonuna keçin. Sonda “Data protection enebled” bölməsinə keçid alaraq parolunuz smartfonunuzda olan məlumatları şifrələyəcək.

Telegram

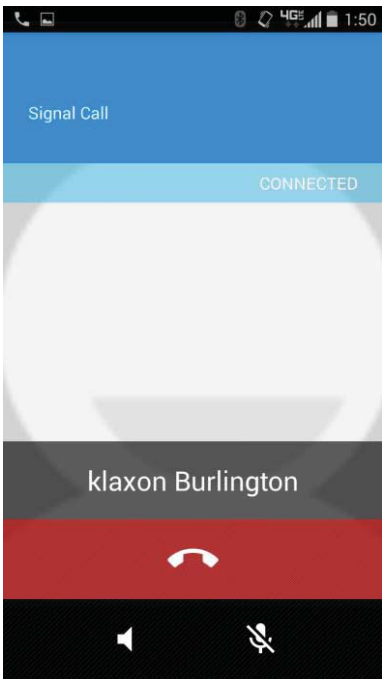


Proqram ödənişsizdir, sürətli və təhlükəsiz yazışma və məlumatların ötürülmə vasitəsi kimi nəzərdə tutulub. Telegramda multichat funksiyası var. Siz burda şəkillərlə videolarla və digər fayllarla həcmi 1Gb keçməmək şərti ilə paylaşa bilərsiniz. Burda təhlükəsiz mesajlaşma və gizli çat funksiyaları da var.

Telegram proqramını telefona qoşma qaydası

1. İnternet mağazadan Telgram əlavəsini yükləyirik.
2. Telefon nömrəmizi geyd edirik. GSM nömrəsini geyd etdikdən sonra SMS-lə kod gəlir. Kodu daxil edərək quraşdırmanı tamamlayırsız.
3. Burada Qrup yazımaları, gizli çat və birbaşa canlı kanal kimi funksiyalar vardır. Setting hissəsindən çatı öz istəyinizə uyğun ayarlıya bilərsiniz.

Telegramın kompüter versiyası da mövcuddur.



Signal

Signal Messenger - Open source tipi IOS və Android telefonları üçün pulsuz proqramdır.

Proqram istfadəçilərin şifrələnmiş grup və fərdi şəkildə mətn mesajları, şəkil və video faylları göndərmək, şifrələnmiş telefon danışıqlarını təmin etmək imkanı verir. Signal telefondakı əlaqə nömrələrini istfadə edərək internet üzərindən bağlantı yaradır.

Signal Messenger proqramını telefona qoşma qaydası

1. İnternet mağazadan əlavəni yükləririk
4. Telefon nömrəmizi geyd edirik. GSM nömrəsini geyd etdikdən sonra SMS-lə kod gəlir. Kodu daxil edərək quraşdırmanı tamamlayırsız.