VUB Informatieveiligheid en Privacy

How To – Veilig thuiswerken

Verantwoordelijke:
Chief Information Security Officer

Contact(en):
ciso@vub.be

Laatste update:
22 maart 2020

© 2020 Vrije Universiteit Brussel

I. Overzicht

Een “How To …” document geeft informatie, hints en tips over een specifiek Informatieveiligheid en Privacy (IVP) onderwerp. Het bevat geen dwingende standaard/richtlijn. Het geeft informatie over hoe een standaard/richtlijn kan toegepast worden.

Het is een ‘levend’ document. De kwaliteit ervan is deels afhankelijk van de feedback van zijn lezers/gebruikers. De cover bladzijde geeft het contact e-mailadres voor het sturen van feedback.

Een “How To” document volgt geen formeel advies- of goedkeuringsproces.

II. Hints en tips over veilig thuiswerken

Als nieuwe VUB-thuiswerker word je uit je comfortzone gehaald. Plotseling ben je geconfronteerd met de organisatorische en technische uitdagingen die eigen zijn aan thuiswerken. Ook als ervaren VUB-thuiswerker stel je je vaak vragen over hoe je veilig kan thuiswerken. De VUB stelt zich tot doel om jou hierin zoveel mogelijk te begeleiden.

Dit document lijst enkele eenvoudige aandachtspunten op om informatieveiligheid bij thuiswerken beter te verzekeren. Deze zullen je niet alleen helpen bij het beveiligen van jouw werk, ze zullen ook jou en je gezin beveiligen in jullie privé internetactiviteiten.

II.1. Vishing en phishing herkennen

Cybercriminelen hebben geleerd dat de gemakkelijkste manier om essentiële gegevens zoals je gebruikersnaam/wachtwoord te verkrijgen, is je ze te vragen. Ze misleiden je zodat je hen deze informatie te goeder trouw geeft. Zij vissen (‘phishing’ in het Engels) naar gevoelige informatie. Dit gebeurt zowel via e-mail (‘phishing)’ als via de telefoon (‘voice phishing’, of ‘vishing’).

Zo kan je opgebeld worden door iemand die zich voordoet als een medewerker van de technische ondersteuning van Microsoft. De medewerker beweert dat je computer is besmet. Je wordt dan gevraagd (kwaadaardige) software te installeren zodat de medewerker je kan helpen. Ook kan je een e-mailwaarschuwing krijgen die meldt dat een pakket niet kon worden afgeleverd. De mail vraagt je om op een (kwaadaardige) link te klikken. Hierdoor wordt kwaadaardige software uitgevoerd.

Dit kan vele vormen aannemen, maar we kunnen een aantal veel voorkomende tactieken terugvinden:

- Veroorzaak een gevoel van urgentie. Vaak worden angst, intimidatie of simulatie van een crisissituatie als hefboom gebruikt om je te overtuigen.
- Boezem vertrouwen in door berichten van een vertrouwde organisatie te vervalsen. Denk bijvoorbeeld aan e-mails die van je banken lijken te komen.
- Zet maximale druk om je ertoe aan te zetten om standaard veiligheidsprocedures te negeren.

Om hiermee ervaring op te doen, kan je de “Leer valse mails herkennen” op Safeonweb raadplegen. Je vindt er tips hoe je een phishing e-mail kan herkennen.

© 2020 Vrije Universiteit Brussel

Uiteindelijk ben jij zelf de beste verdediging tegen deze aanvallen.

II.2. Je thuisnetwerk beveiligen

De meeste thuisnetwerken gebruiken een draadloze verbinding of wifi. Dit is vergelijkbaar met het VUBNext wifinetwerk op de campus. De VUB beschermt haar wifinetwerken tegen allerhande aanvallen. Het is echter even belangrijk dat ook jij jouw wifinetwerk thuis voldoende goed beveiligt. Wanneer iemand met kwade bedoelingen zomaar op jouw netwerk verbonden geraakt, kan deze heel wat schade aanrichten omdat in de regel alle toestellen die op het netwerk zijn verbonden als veilig worden beschouwd.

Het centrale punt van je wifinetwerk is de router. Dit apparaat communiceert met je eigen toestel door wifisignalen. Iedere router kan ingesteld worden. De procedure om dat te doen verschilt van router tot router. Er zijn echter een paar instellingen die je voor alle wifinetwerken terugvindt. Kies steeds voor een stevig wachtwoord en kies ook voor een veilige communicatie zoals WPA2 voor je wifinetwerk.

Weet je niet zeker hoe je deze stappen moet uitvoeren? Vraag het dan aan je internetprovider, bezoek de help pagina's of de FAQ's, en controleer de documentatie die ofwel bij je router is geleverd ofwel verwijst naar de website van de leverancier.

II.3. Gebruik een Virtual Private Network (VPN).

De VUB biedt een veilige verbinding tot de interne VUB-systemen aan als je je niet op de campus bevindt. De VUB gebruikt hiervoor een Virtueel Privé Netwerkoplossing (Engels: Virtual Private Network). Deze software zorgt voor een beveiligde verbinding tussen jouw toestel en het VUB-netwerk. Alle communicatie verloopt door een versleutelde virtuele tunnel, die vermijdt dat cybercriminelen leesbare communicatie kunnen onderscheppen en zo de informatie kunnen bemachtigen.

De VUB vereist dat alle communicatie die van buiten het VUB-netwerk vertrekt om toestellen te bereiken die verbonden zijn op het interne VUB-netwerk, over de VUB-VPN loopt. Dit betekent echter niet dat je voor alle thuiswerkactiviteiten een VUB-VPN-verbinding nodig hebt. De VUB biedt immers meerdere diensten aan die rechtstreeks beschikbaar zijn op het internet. Zo kunnen o.a. Office-365 (OneDrive, SharePoint, e-mail, …), de helpdesk portal via ServiceNow, TEO, PAM, Owncloud, Canvas, CaLi, Pure en Ultimo rechtstreeks zonder VPN bereikt worden.

Heb je toegang nodig tot een meer beveiligde dienst van de VUB, dan gebruik je de Pulse Secure VPN-software die aangeboden wordt door de VUB. Heb je deze software nog niet geïnstalleerd, raadpleeg dan de "VPN-toegang via Pulse Secure" installatiehandleiding die je kan terugvinden op de VUB-helpdesk portaal.

Vergeet niet dat je dit pakket enkel kan gebruiken als je een geregistreerd VUB-VPN gebruiker bent. Je kan de registratie heel eenvoudig aanvragen via de "Nieuwe VPN-account" item op het helpdesk-portaal.

© 2020 Vrije Universiteit Brussel

II.4. Gebruik sterke wachtwoorden

Een stevig wachtwoord is steeds de eerstelijnsbeveiliging van je systeem. Gebruik voor elke gelegenheid een verschillend wachtwoord: eentje voor je toestel, een ander voor je wifinetwerk, nog een ander voor je Facebook, voor je Gmail, enzovoort…

Je toegang tot alle VUB-systemen bekom je met één enkele VUB-gebruikersnaam en wachtwoord. De meerderheid van de centrale VUB-applicaties die je via je browser benadert gebruiken een eenmalig aanmeldingsproces (Engels: single sign-on of SSO). Hierdoor hoef je om toegang te verkrijgen tot al je VUB-systemen maar éénmaal in te loggen. Van zodra je je browser sluit, sluit je je connectie af en hiermee vervalt je eenmalig aanmeldingsproces. Momenteel zijn enkel RACS en EasyPay, Pure en CaLi als centrale VUB-applicaties nog niet aangesloten op deze SSO.

We benadrukken nogmaals om nooit je VUB-wachtwoord met andere personen te delen, en om voor elke verschillende dienst (VUB, Gmail, Facebook, ..) een ander wachtwoord te gebruiken. Overweeg het gebruik van een wachtwoordmanager om al je persoonlijke wachtwoorden te beheren, maar ook daar sla je best je VUB-wachtwoord niet in op.

Lees zeker de “How To – Wachtwoord beheer” op de Informatieveiligheid en Privacy website.

II.5. Voer updates tijdig uit

Cybercriminelen zijn steeds op zoek naar kwetsbaarheden in de software die je toestel gebruikt. Dit geldt niet alleen voor de software van je laptop of desktop, maar ook voor de software van je op het internet aangesloten televisie, babyfoon, beveiligingscamera, router voor thuisgebruik, gameconsole, … Algemeen geldt dat voor alle technologie die kan verbonden worden met het internet.

De leveranciers van deze systemen brengen regelmatig updates uit om de tekortkomingen in hun software te verhelpen. Deze brengen niet alleen nieuwe functionaliteiten naar je systeem, maar dichten ook gekende kwetsbaarheden die je informatieveiligheid in gevaar brengen. Het is dan ook uiterst belangrijk dat je deze updates steeds installeert, liefst met een automatische updatefunctie indien deze voorhanden is. Let hierbij vooral goed op dat je enkel officiële leveranciersbronnen voor deze updates gebruikt!

Uiteraard verschijnt de “update gereed om te installeren” melding altijd wanneer je net serieus aan het werken bent. Je wil dan je computer zeker niet heropstarten, en dus klik je de melding weg. Besef dat je het hierdoor voor cybercriminelen veel gemakkelijker maakt om je systeem te hacken. Het succes van de cybercriminaliteit wordt gevoed door de race tussen cybercriminelen en updates. Klik het bericht dus niet weg, installeer de update van zodra hij beschikbaar wordt en maak van de nood een deugd: neem een korte pauze tijdens de installatie van de update.

Software die niet meer ondersteund wordt door de leverancier krijgt ook geen beveiligingsupdates meer. Oude besturingssystemen zoals bijvoorbeeld Windows XP of Windows 7, oude e-mailprogramma’s, of elke andere software die niet langer ondersteund wordt vormt een zeer belangrijk beveiligingsrisico. Het is daarom niet toegestaan om niet-ondersteunde software te gebruiken. Uitzonderingen kunnen gemaakt worden voor systemen waar een vervanging onmogelijk of te duur is, maar dit moet dan gepaard gaan met afdoende risico limiterende maatregelen. Ben je verantwoordelijk voor een dergelijk systeem, check dan steeds wat er moet

© 2020 Vrije Universiteit Brussel

ondernomen worden met je Chief Information Security Officer, ciso@vub.be, en doe dat altijd vóór je de niet meer ondersteunde software blijft gebruiken.

II.6. Veilig communicatiekanalen gebruiken

Communicatiemiddelen zijn belangrijk bij het thuiswerken. Zoals we hierboven al zagen laat de VUB-VPN je toe om je van thuis uit op het VUB-netwerk aan te sluiten. Maar er zijn ook nog heel veel andere communicatiemiddelen. Wat van heel groot belang is, is dat je een heel duidelijk onderscheid maakt tussen privé en werkcommunicatie en dat je deze vooral niet mengt. Voor je werkcommunicatie gebruik je best enkel applicaties die door de VUB geselecteerd werden.

Voor individuele of groepsgesprekken gebruik je eventueel Skype voor Business of liever het recenter in gebruik genomen Microsoft Teams. Je kan beide applicaties samen met je besturingssysteem laten opstarten. Je dient dit te selecteren in de settings van beide applicaties. Dan kunnen je collega's je steeds via deze applicaties contacteren. Gebruik geen andere applicaties voor werkgesprekken. Skype for business en Teams voldoen beiden aan de veiligheidsvereisten van de VUB. Voor de alternatieve applicaties is dit echter niet zeker.

Verstuur je e-mail voor je werk, dan gebruik je enkel je VUB-account. Soms lijkt het handig om snel een bestandje naar je eigen Gmail account te sturen zodat je het document lokaal kan afprinten, of indien je printer het ondersteunt je document rechtstreeks naar je lokale printer te e-mailen. Denk eraan dat hierdoor VUB-informatie verspreid wordt over meerdere locaties. Deze locaties voldoen echter niet altijd aan de VUB-veiligheidsvereisten, en kunnen leiden tot het lekken van gevoelige informatie. Doe dit dus in geen geval! Gebruik enkel je lokale printer als die aan je systeem is gekoppeld zodat je rechtstreeks kan printen.

Surf je naar websites, let er dan op dat je browser steeds een HTTPS en geen HTTP-verbinding gebruikt. Doe dit zeker als je persoonlijke gegevens op die website moet ingeven, zoals je gebruikersnaam en wachtwoord. HTTPS gebruikt een versleutelde en beveiligde communicatie. Dit is niet het geval voor een HTTP-verbinding, waarbij al jouw ingevoerde gegevens integraal en zonder versleuteling over het internet verstuurd worden en die bijgevolg door cybercriminelen onderschept kunnen worden.

Om je thuiswerk te ondersteunen kunnen sommige collega's je hun (private) mobiel nummer doorgeven. Denk eraan dat je dit nummer enkel krijgt voor werkgerelateerde communicatie. Gebruik het nummer niet voor andere doeleinden en verspreid het zeker niet, behalve als je collega je hiervoor expliciet toestemming geeft.

Bij thuiswerken is de grens tussen gebruik van je (privé) sociale media en werkactiviteiten minder vanzelfsprekend dan op het kantoor. Het online zetten van kleine werkdetails of je dagelijkse routine lijkt minder raar als er geen collega's zijn waarmee je die dingen kan delen. Thuiswerkers moeten hiermee toch oppassen, want zo'n updates bieden vaak waardevolle informatie voor het opzetten van phishing-campagnes.

II.7. Zorg voor een up-to-date antivirus

Je systeem moet een actieve en up-to-date antivirus hebben, die automatisch de virus-updates installeert. Dit is onontbeerlijk voor de veiligheid van je systeem.

© 2020 Vrije Universiteit Brussel

De VUB biedt al zijn werknemers en studenten McAfee Endpoint Security aan. Je kan hier McAfee installatie instructies vinden.

II.8. Bescherm je werksysteem ook voor kinderen en gasten.

Op kantoor hoef je je geen zorgen te maken over kinderen, gasten of andere gezinsleden die je werklaptop of je eigen systemen waarmee je voor de VUB werkt gebruiken. Draag er zorg voor dat bij thuiswerken het duidelijk maakt voor familie en vrienden dat ze je werksystemen niet (altijd) kunnen gebruiken. Dit gebruik leidt tot een ernstig risico: VUB-informatie kan per ongeluk gewist of gewijzigd worden, of het systeem kan in het ergste geval per ongeluk geïnfecteerd geraken.

II.9. Finaal: gebruik steeds je gezond verstand

Uiteindelijk wordt van elke medewerker verwacht dat deze zijn/haar gezond verstand gebruikt om veilig te kunnen thuiswerken. En indien er vragen zijn, aarzel dan zeker niet om deze te stellen. Stuur bij twijfel een e-mail naar helpdesk@vub.be met je vragen: onze helpdesk staat steeds paraat om je te ondersteunen voor veilig thuiswerk.

© 2020 Vrije Universiteit Brussel