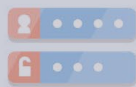


23 JUNI 2021



Introductie security awareness

Wat is het belang van veiligheidsbewustwording en wat zijn de risico's en consequenties van menselijk handelen?



Sterke wachtwoorden

Informatiebeveiliging begint met een sterk wachtwoord. Hoe kan men sterke wachtwoorden maken die makkelijk te onthouden zijn?



Veilig surfen op internet

We surfen dagelijks op internet. Hoe kan men veilig surfen op internet?



De beveiligde verbinding

Waarom is een beveiligde verbinding (HTTPS) zo enorm belangrijk?



Informatie in de cloud

We werken steeds vaker in de cloud. Hoe maakt men veilig gebruik van cloud-diensten?



De grootste gevaren op internet

Gevaren liggen overal op de loer. Wat is cybercriminaliteit en welke gevaren zijn er?



Phishing

De grootste digitale dreiging waar organisaties mee te maken hebben. Wat is phishing, hoe kan men phishing herkennen en hoe dient men te reageren?



De veilige computer

De computer is onmisbaar. Wat moet men wel en niet doen om veilig gebruik te maken van de computer en hoe houdt men deze virusvrij?



De veilige werkplek

Hoe draagt men bij aan een veilige werkplek, waarin zorg...



Datavernietiging

Informatie is goud waard.



Social engineering

Hoe herkent men social...



Beveiliging van mobiele apparaten

We nemen ze overal mee naar toe. Hoe gaat men op de juiste manier met mobiele apparaten om en hoe gaat men voor een adequate beveiliging?

SECURITY AWARENESS IN 6 STAPPEN

Creëer een security bewuste organisatie in 6 stappen.

Met dit stappenplan geven wij je de juiste handvatten om je bedrijf en medewerkers bewust te maken over het belang van security awareness.

Wifi

Hoe kan men veilig buiten de deur werken en hoe kan men veilig gebruik maken van wifi?



Veilig apps downloaden

We maken veel gebruik van apps op onze mobiele apparaten. Hoe weet men of een app veilig is?

USB-opslagapparaten

Het gemak van USB-opslagapparaten is groot, maar brengt ook risico's met zich mee. Hoe gaat men veilig met deze apparaten om?



Privacy

Hoe moet men omgaan met persoonlijke data in het dagelijks werk? Welke gegevens mogen er uitgewisseld worden en welke niet?



1. CREËER BEWUSTWORDING / DRAAGVLAK

Medewerkers zijn zich vaak niet bewust van de belangrijke rol die zij vervullen binnen de informatiebeveiliging van hun organisatie. Helaas gebeurt het erg vaak dat mensen klikken op links in phishingmails (met alle gevolgen van dien) of onbewust gevoelige informatie delen. De medewerkers scherp krijgen op het gebied van informatiebeveiliging is van groot belang! Een goede start om bewustwording te creëren is een gecoördineerde phisingsimulatie. Hiermee krijg je inzicht in de huidige situatie, hoe alert je medewerkers zijn en of een training zinvol of noodzakelijk is.

Hoe werkt een phisingsimulatie?

Medewerkers ontvangen een e-mail met een veilige 'besmette' link en diverse andere phishing kenmerken. Vervolgens wordt gemeten wat men doet...klikt men of denkt men even na? Afhankelijk van wat men doet volgen er tips en advies, een moment van bewustwording! Je medewerkers zullen voortaan alerter zijn bij het openen van dubieuze e-mails. Met de rapportage van de simulatie kun je advies inwinnen over de mogelijke stappen ter verbetering van de security awareness bij je medewerkers.



“De totale schade door phishing in 2020 was ruim 60% hoger dan in 2019!”

2. SECURITY AWARENESS TRAINING

Na de meting uit stap 1 heb je precies in beeld welke kennis je medewerkers hebben of nog nodig hebben. Met deze informatie kun je een passend trainingsplan ontwikkelen.

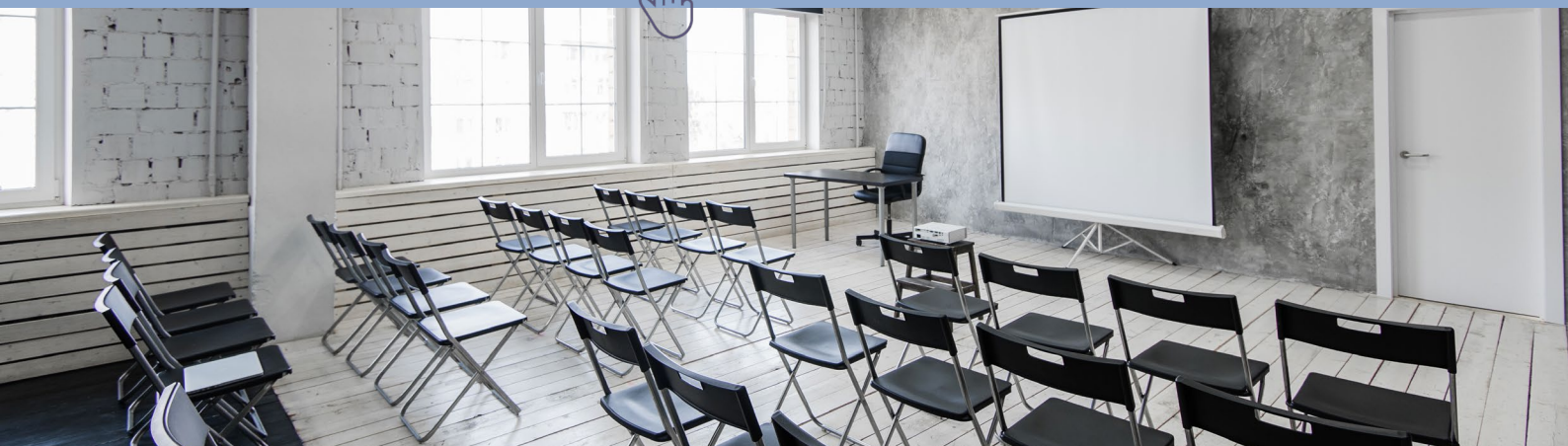
De sterkste schakel ben jij en je medewerkers

Security Awareness is belangrijker dan ooit! Creëer veranderingen in bewustzijn en gedrag op het gebied van informatiebeveiliging, cybersecurity en privacy. Onderzoek het gedrag van medewerkers, geef inzicht in de huidige beveiligingsniveaus en train medewerkers. Zo maak je van je medewerkers de sterkste schakel in informatiebeveiliging en creëer je een veilige werkomgeving.

Maar hoe doe je dit?

Wij bieden hiervoor ons security awareness trainingsplatform. Hét platform voor online security awareness training. Ons trainings- en phishingplatform is de perfecte tool om medewerkers doorlopend te trainen op het gebied van security awareness. Verhoog het veiligheidsbewustzijn, activeer de human firewall en bescherm jouw organisatie tegen beveiligingsrisico's. In overleg stellen wij een op maat gemaakt trainingsprogramma beschikbaar. Wij richten het complete platform voor je in en bewaken de voortgang. De voortgang wordt teruggekoppeld aan het management. Je hebt hier geen werk aan, maar integreert wel een op maat gemaakt trainingsprogramma.

Benieuwd naar de mogelijkheden? [Klik hier!](#)



3. ZORG VOOR DUIDELIJKE AFSPRAKEN

‘Mijn ICT-partner heeft dit allemaal geregeld...’ is een vaak gehoorde reactie wanneer we het hebben over back-ups, herstelplannen en zaken rondom de ICT omgeving. Maar weet je dit wel zeker? Worden je back-ups regelmatig gecontroleerd? Is er een herstelplan aanwezig? Zo ja, wie voert dit uit bij calamiteiten? Hoe lang duurt het voordat je je gegevens weer terug krijgt? Zo maar een paar vragen die je met zekerheid zou moeten kunnen beantwoorden.

Het is van belang dat je beschikt over goede documentatie van je ICT omgeving. Zorg er ook voor dat je toegang hebt tot deze documentatie. Zorg voor een herstelplan waarin duidelijk staat beschreven wie verantwoordelijk is voor het herstel bij calamiteiten en hoe lang dit mag duren. Klinkt allemaal logisch. Helaas gebeurt dit in de praktijk nog te weinig.

4. ANALYSEER JE ICT OMGEVING

Vandaag de dag is het voorkomen van een hack of een datalek essentieel voor organisaties, relaties en klanten. Een volledig vertrouwen op veilige online data en de naleving van wet- en regelgeving is essentieel voor elke organisatie.

Digitalisering en data zijn de drijvende kracht maar brengen veel risico's met zich mee voor informatiebeveiliging en data-eigendom. Al deze vertrouwelijke informatie is natuurlijk interessant voor cybercriminelen. Voorbereid zijn op de grootste cyberrisico's is nu een dagelijkse handeling. Bedenk wat er gebeurt als de informatie die je organisatie nodig heeft niet beschikbaar is, je niet kunt werken of belangrijke gegevens in handen vallen van cybercriminelen. Het is uiterst belangrijk om deze cybercriminelen een stap voor te blijven en dat begint bij inzicht krijgen in de zwakke punten van je ICT-omgeving. Een security scan geeft je dit inzicht en toont aan wat je moet doen om optimaal veilig te kunnen werken. Een security scan is niet kostbaar maar levert je veel op; veiligheid, gemoedsrust en vertrouwen bij je relaties.

Benieuwd naar de mogelijkheden? [Klik hier!](#)



5. ZORG DAT JE DATA VEILIG STAAT

Het klinkt vanzelfsprekend en je hoort dit vast niet voor de eerste keer: “**Zorg voor een goede back-up!**”. Maar wat is een goede back-up? Eigenlijk wil je je hiermee niet bezig houden, je wilt je tenslotte focussen op je eigen werk en dagelijkse bedrijfsvoering. Mocht je onverhoopt iets kwijtraken wil je je ICT-partner kunnen bellen, zodat zij het bestand terug kunnen halen...klinkt simpel, toch? Helaas zien we nog te vaak dat bedrijven geen idee hebben van hoe hun back-up in elkaar steekt of erger nog, ze weten niet eens of er wel een back-up is! Daarnaast is er ook nog de verwarring dat veel mensen die werken in de Cloud, denken dat een back-up automatisch is inbegrepen. Soms is dit zo maar vaak ook niet. En voldoet de inbegrepen oplossing wel aan je eisen? Overleg met je ICT partner en zorg dat hij je een goede back-up kan garanderen.

Hierbij een paar tips die bijdragen aan een goede back-up:

- Zorg voor een goede frequentie;
- Laat je back-ups controleren en voer periodiek restore testen uit;
- Zorg ervoor dat je gegevens op meerdere locaties zijn opgeslagen;
- Lees meer op [onze website](#) of [neem contact met ons op!](#)



6. MAAK VAN SECURITY AWARENESS EEN PROCES

Security Awareness moet een proces worden binnen je bedrijf. Periodiek trainen, simuleren en toetsen is belangrijk om je medewerkers scherp te houden.

Wij komen graag met je in contact en helpen je om de kans op cyberaanvallen te minimaliseren!
[Neem contact met ons op!](#)



OVER UNITIT SOLUTIONS B.V.

UnitIT is een meedenkende, probleemoplossende partner die organisaties helpt grip te houden op hun ICT. Hierdoor kunnen deze succesvoller zijn, omdat ze zich optimaal kunnen richten op hun kernactiviteiten, ICT dient immers altijd en overal beschikbaar te zijn.

Onze innovatieve en energievriendelijke oplossingen, ingericht volgens 'best practice' en beheerd door onze gecertificeerde medewerkers (o.a. Microsoft Certified) en beproefde procedures (o.a. ITIL), garanderen een optimaal beveiligde en beschikbare ICT-omgeving.

Onze handelwijze kenmerkt zich door een proactieve houding en het ontzorgen van de klant door verantwoordelijkheid te nemen over uw ICT.

VEILIGHEID

BESCHIKBAARHEID

PRIVACY

WIJ BELOVEN: FIRST CLASS ICT
UW CONTINUÛTEIT IS ONZE ZORG!



UnitIT Solutions BV
Joulehof 5-7
4622 RG Bergen op Zoom
(The Netherlands)

Telefoon: +31(0)164 27 55
E-mail: info@unitIT.nl
Website: www.unitIT.nl
KvK dossiernr.: 220.39479