

ΨΗΦΙΑΚΑ ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ

ΤΑΞΗ Γ

ΣΧΟΛΙΚΟ ΕΤΟΣ 2021 - 2022

ΨΗΦΙΑΚΑ ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ

ΚΕΦ	ΤΙΤΛΟΣ	ΣΕΛΙΔΑ
1ο	Εισαγωγή	3
2ο	Οι αλλαγές που φέρνει ο Κώδικας Ψηφιακής Διακυβέρνησης	4
3ο	Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025	9
4ο	Ασφάλεια Ηλεκτρονικών Συναλλαγών	12
5ο	Συμπεράσματα	21

Εισαγωγή

Το τελευταίο στάδιο της επανάστασης της πληροφορικής είναι στο επίπεδο του πολίτη.

Η επανάσταση στις επικοινωνίες/τηλεπικοινωνίες έφερε τον κόσμο σε νέα πραγματικότητα. Η επικοινωνία των ανθρώπων μηδενίστηκε ως προς την απόσταση και την ταχύτητα. Οι άνθρωποι επικοινωνούν με άλλους ανθρώπους σε πραγματικό χρόνο σε κάθε σημείο του πλανήτη. Επίσης μπορούν να ανταλλάσσουν στοιχεία και έγγραφα ηλεκτρονικά σε ελάχιστο χρόνο.

Πρώτοι που το εκμεταλλεύτηκαν αυτό ήταν οι εταιρείες, πληροφορικής και άλλες, συμπεριλαμβανομένων τις τράπεζες. Ακολούθησαν τα κράτη που οργάνωσαν τα αρχεία τους όσον αφορά τις δικές τους δομές. Ακολούθησε η ψηφιακή επικοινωνία κράτους επιχειρήσεων. Τώρα στην Ελλάδα είμαστε στο στάδιο που ο πολίτης και το κράτος επικοινωνούν και αλληλεπιδρούν ψηφιακά, με την πανδημία του covid-19 να δίνει μεγάλη ώθηση σε αυτό.

Βεβαίως υπάρχει μεγάλη αλληλεπίδραση μεταξύ επιχειρήσεων και πολιτών, το οποίο αυξάνονταν αναλογικά με την ψηφιακή οικειοποίηση των πολιτών. Ένας από τους βασικούς παράγοντες που βοήθησε αυτό είναι το κινητό τηλέφωνο αφής. Οι διαδικτυακές αγορές αυξάνονταν όσο αυξάνονταν οι διαδικτυακοί πελάτες. Ο covid-19 βοήθησε επίσης στο να ωθήσει επιπλέον ομάδες πληθυσμού στην ψηφιακή εκμάθηση και στο διαδικτυακό εμπόριο.

Με όλα αυτά τα νέα δεδομένα οφείλουμε να γνωρίζουμε τις ψηφιακές υποχρεώσεις και δικαιώματά. Νέοι νόμοι από το κράτος και την Ευρωπαϊκή Ένωση υπάρχουν όπως και Ευρωπαϊκές οδηγίες, ώστε να βάλουν μια τάξη στο διαδίκτυο γενικότερα.

Εκτός από τους νόμους θα πρέπει οι πολίτες να αυτοπροστατευτούν από απάτες, κακόβουλα λογισμικά, τα πνευματικά τους δικαιώματα, τα προσωπικά τους δεδομένα, το ψηφιακό bullying και την προσωπική τους ζωή. Πέρα από τους νόμους και τις οδηγίες της Ευρωπαϊκής Ένωσης, ο πολίτης οφείλει να προσέχει και να προστατεύεται γιατί σε πολλές περιπτώσεις τα ψηφιακά εγκλήματα δεν ταυτοποιούνται ή βρίσκονται σε περιοχές έξω από την δικαιοδοσία της Ευρωπαϊκής Ένωσης, με αποτέλεσμα να μην μπορεί να δικαιωθεί ή να αποζημιωθεί ο πολίτης.

Τα παραπάνω είναι τα βασικά σημεία που θα διαπραγματευτή η εργασία αυτή.

Οι αλλαγές που φέρνει ο Κώδικας Ψηφιακής Διακυβέρνησης

<https://www.fortunegreece.com/article/i-allages-pou-ferni-o-kodikas-psifiakis-diakivernisis/>

Σημαντικές αλλαγές στη ζωή των Ελλήνων φέρνει ο Κώδικας Ψηφιακής Διακυβέρνησης που πρόκειται να τεθεί σε διαβούλευση στην Βουλή τις επόμενες ημέρες. Νέες συνήθειες, λιγότερες διαδικασίες και κυρίως λιγότερη γραφειοκρατία υπόσχεται το νέο νομοσχέδιο, στο οποίο μεταξύ άλλων, προωθείται νομοθετικό πλαίσιο για τον Ενιαίο Αριθμό του Πολίτη, τις ψηφιακές υπογραφές, τις ψηφιακές σφραγίδες, τα ψηφιακά έγγραφα.

Για τη χρησιμότητα και τον κομβικό ρόλο του Κώδικα μίλησε ο υπουργός Ψηφιακής Διακυβέρνησης, Κυριάκος Πιερρακάκης υπογραμμίζοντας ότι «όταν ξεκινήσαμε να σχεδιάζουμε την ψηφιακή μας στρατηγική, διαπιστώσαμε άμεσα ότι, πέρα από τις αναγκαίες νομοθετικές τομές, εξίσου απαραίτητη ήταν και η κωδικοποίηση του υπάρχοντος πλαισίου, ώστε όλοι να γνωρίζουν με σαφήνεια τι ισχύει. Δεν θέλαμε να υπάρξει ούτε ένα περιστατικό άρνησης εξυπηρέτησης από δημόσια υπηρεσία, επειδή δεν είχε φτάσει κάποια ερμηνευτική εγκύκλιος. Σε αυτά τα δύο ζητούμενα έρχεται να δώσει απαντήσεις ο Κώδικας Ψηφιακής Διακυβέρνησης: στην επικαιροποίηση και την ενοποίηση της νομοθεσίας σχετικά με την ψηφιακή διακυβέρνηση».

Και ο γενικός γραμματέας Ψηφιακής Διακυβέρνησης και Απλούστευσης Διαδικασιών, Λεωνίδας Χριστόπουλος, για το ίδιο θέμα, τόνισε ότι «ο Κώδικας Ψηφιακής Διακυβέρνησης είναι το απαραίτητο θεσμικό πλαίσιο για τον ψηφιακό μετασχηματισμό τόσο του κράτους, όσο και της κοινωνίας ευρύτερα. Είναι ένα νομοσχέδιο που θέτει τις βάσεις για την περαιτέρω ανάκτηση της εμπιστοσύνης των πολιτών στο κράτος και τη δημόσια διοίκηση. Παράλληλα, έχει έντονα αναπτυξιακό χαρακτήρα, υπακούοντας, την ίδια στιγμή, στις αρχές της προστασίας των προσωπικών δεδομένων των πολιτών. Θεωρούμε, ότι με το νομοσχέδιο αυτό, το Επιτελικό συναντά το Ψηφιακό Κράτος, δημιουργώντας μια νέα, θετική δυναμική στις σχέσεις κράτους-πολίτη. Έρχεται, άλλωστε, να βελτιώσει ριζικά τον τρόπο που οι πολίτες συναλλάσσονται με το Δημόσιο, αλλά και την εσωτερική επικοινωνία και οργάνωση του Δημοσίου».

Αναφερόμενος, ο κ. Πιερρακάκης, στις ψηφιακές υπηρεσίες που είχαν θεσμοθετηθεί με ΠΝΠ για την αντιμετώπιση των συνεπειών της κρίσης της

COVID-19, επεσήμανε ότι «σε αυτή τη νομοθετική πρωτοβουλία τις μονιμοποιούμε. Πρόκειται για ένα εργαλείο που θα βοηθήσει την Ελλάδα να προχωρήσει γρήγορα στον ψηφιακό μετασχηματισμό και ταυτόχρονα θα της επιτρέψει να προσαρμόζεται εύκολα στα νέα δεδομένα που θα ανακύπτουν. Έτσι, με μια σειρά από διατάξεις σχετικά με τον Προσωπικό Αριθμό, τις ψηφιακές υπογραφές, τις ψηφιακές σφραγίδες και τα ψηφιακά έγγραφα, που θα αλλάξουν ριζικά τις σχέσεις κράτους-πολίτη, αυξάνοντας την ταχύτητα και θωρακίζοντας τα προσωπικά δεδομένα. Επιπλέον, με την ενσωμάτωση των ευρωπαϊκών οδηγιών για τα ανοιχτά δεδομένα και του Κώδικα Ηλεκτρονικών Επικοινωνιών της ΕΕ ανοίγουμε τον δρόμο για την τεχνολογική εξέλιξη της χώρας. Και τέλος, με αναπτυξιακές διατάξεις όπως το cloud first policy απελευθερώνουμε τις τεχνολογικές δυνατότητες της Δημόσιας Διοίκησης και μειώνουμε τη γραφειοκρατία προς πολίτες και επιχειρήσεις, που θα οδηγήσουν σε ενδυνάμωση του ΑΕΠ της χώρας».

Συγκεκριμένα, οι επτά πιο σημαντικές καινοτομίες που αφορούν άμεσα τον πολίτη είναι:

1. Θεσμοθέτηση Προσωπικού Αριθμού (ΠΑ) για τους πολίτες

α) Καθιερώνεται προσωπικός αριθμός (ΠΑ) για την ταυτοποίηση των φυσικών προσώπων, με σκοπό την παροχή υπηρεσιών από φορείς του δημόσιου και του ευρύτερου δημόσιου τομέα. Ο ΠΑ αποδίδεται δε μία φορά στο φυσικό πρόσωπο και δεν μεταβάλλεται.

β) Ο ΠΑ αποδίδεται σε κάθε φυσικό πρόσωπο που δικαιούται Αριθμό Φορολογικού Μητρώου (ΑΦΜ) ή Αριθμό Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ). Σε όσα φυσικά πρόσωπα έχει αποδοθεί ΑΦΜ, αυτός αποτελεί τον ΠΑ. Σε όσα φυσικά πρόσωπα έχει αποδοθεί μόνο ΑΜΚΑ, τους αποδίδεται ο ΠΑ σύμφωνα με διαδικασία που ορίζεται σε απόφαση.

γ) Ο ΠΑ δεν συνεπάγεται αυτοδικαίως τη χορήγηση δικαιωμάτων ή την επιβολή υποχρεώσεων στον κάτοχό του. Οι όροι και οι προϋποθέσεις για τα δικαιώματα και υποχρεώσεις του κατόχου του ΠΑ ρυθμίζονται από την κείμενη φορολογική, εργατική και ασφαλιστική νομοθεσία.

δ) Ο ΠΑ θα αντικαταστήσει τον ΑΦΜ των φυσικών προσώπων και τον ΑΜΚΑ σταδιακά και με πλήρη αντικατάσταση εντός μιας διετίας

2. Θεσμοθέτηση ηλεκτρονικής υπηρεσίας συστημένης παράδοσης

Εισάγεται η ηλεκτρονική υπηρεσία συστημένης παράδοσης: ό,τι αποτελεί το σημερινό συστημένο ταχυδρομείο, μπορεί να αποτελέσει η υπηρεσία συστημένης παράδοσης για τον ηλεκτρονικό κόσμο. Στόχος να αποτελέσει ένα ασφαλές ηλεκτρονικό «κανάλι επικοινωνίας» του Δημοσίου με τους πολίτες

και τις επιχειρήσεις. Μέχρι τώρα η ως άνω υπηρεσία, μολονότι προβλεπόταν στον ευρωπαϊκό κανονισμό, παρέμεινε αναξιοποίητη. Με τον Κώδικα Ψηφιακής Διακυβέρνησης δημιουργούνται οι συνθήκες για να αναπτυχθεί τόσο στο ιδιωτικό όσο και στον δημόσιο τομέα. Ειδικότερα, στο Δημόσιο παρέχονται νέες δυνατότητες ηλεκτρονικής διεπαφής Δημοσίου και πολιτών/επιχειρήσεων. Στόχος ο διοικητικός έλεγχος να γίνεται ηλεκτρονικά.

3. Θεσμοθέτηση Μητρώου Διοικητικών Διαδικασιών Δημοσίου

Στο Μητρώο αυτό καταχωρούνται όλες οι ψηφιακές ή φυσικές διαδικασίες του Δημοσίου τομέα ανεξαρτήτως εάν αφορούν παροχή δημόσιας υπηρεσίας σε πολίτες ή φορείς του ιδιωτικού τομέα ή εσωτερικές διαδικασίες του δημοσίου τομέα. Ουδεμία παρέκκλιση δεν μπορεί να υπάρξει κατά την εφαρμογή της διαδικασίας από οποιαδήποτε αρμόδια υπηρεσία του Δημοσίου. Αυτό σημαίνει ότι ο πολίτης μπορεί να γνωρίζει με βεβαιότητα τη διαδικασία που απαιτείται για τη συναλλαγή του με το Δημόσιο χωρίς να εκτίθεται σε φαινόμενα αυθαιρεσίας και περιττής γραφειοκρατίας.

4. Θεσμοθέτηση Μητρώου Επικοινωνίας Πολιτών

Αποτελεί το μοναδικό σημείο της Δημόσιας Διοίκησης, όπου ο πολίτης θα δηλώνει τα στοιχεία επικοινωνίας του (διεύθυνση, τηλέφωνο, email). Όλοι οι δημόσιοι φορείς θα χρησιμοποιούν αποκλειστικά αυτό το μητρώο, για να ενημερώνονται για τα στοιχεία επικοινωνίας των πολιτών, χωρίς να απαιτείται οι πολίτες να δηλώνουν ή να επικαιροποιούν ξεχωριστά σε κάθε φορέα τα στοιχεία επικοινωνίας τους.

5. Ενδυνάμωση της Ενιαίας Ψηφιακής Πύλης (gov.gr)

Το νέο εργαλείο για την πραγματική ψηφιακή διακυβέρνηση, η αποκλειστική πύλη παροχής ψηφιακών υπηρεσιών προς πολίτες/επιχειρήσεις, θεσπίστηκε με το άρθρο 52 του ν. 4635/2019. Πλέον, εισάγονται περαιτέρω ρυθμίσεις για τη λειτουργία της, βασικά στοιχεία: δυνατότητα έκδοσης εγγράφων/αιτήσεων από φυσικά πρόσωπα, ισχυρές μέθοδοι αυθεντικοποίησης ώστε να υπάρχει η μέγιστη βεβαιότητα για την ταυτότητα του φυσικού προσώπου που χρησιμοποιεί κάθε υπηρεσία)

6. Υποχρέωση παροχής ψηφιακών δημοσίων υπηρεσιών κάτω από την ομπρέλα της ΕΨΠ (gov.gr)

Η Ενιαία Ψηφιακή Πύλη της Δημόσιας Διοίκησης (gov.gr – ΕΨΠ) αποτελεί την αποκλειστική πύλη παροχής ψηφιακών δημοσίων υπηρεσιών προς πολίτες/επιχειρήσεις. Εισάγονται περαιτέρω ρυθμίσεις για τη λειτουργία της με βασικά στοιχεία τη δυνατότητα έκδοσης εγγράφων/αιτήσεων από φυσικά ή νομικά πρόσωπα και την καθιέρωση ισχυρών μεθόδων επαλήθευσης

της ταυτότητας του συναλλασσομένου προσώπου (αυθεντικοποίηση), ώστε να υπάρχει η μέγιστη βεβαιότητα για την ταυτότητα του προσώπου που χρησιμοποιεί κάθε υπηρεσία.

7. Μονιμοποίηση των νέων ψηφιακών υπηρεσιών που είχαν θεσμοθετηθεί με ΠΝΠ για την αντιμετώπιση των συνεπειών της κρίσης της COVID-19
Κωδικοποιούνται οι διατάξεις της από 20.3.2020 ΠΝΠ για τις πρώτες ψηφιακές δημόσιες υπηρεσίες μέσω της ΕΨΠ:

α) Ηλεκτρονική υπεύθυνη δήλωση

β) Ηλεκτρονική εξουσιοδότηση

γ) άυλη συνταγογράφηση

δ) Εφεξής, δεν απαιτείται η φυσική παρουσία του πολίτη στις αρμόδιες αρχές για την επικύρωση του γνήσιου της υπογραφής σε υπεύθυνες δηλώσεις και εξουσιοδοτήσεις, καθώς η αυθεντικοποίηση που πραγματοποιείται για τη χρήση των ψηφιακών δημόσιων υπηρεσιών της ΕΨΠ έχει την ίδια ισχύ με την βεβαίωση γνήσιου υπογραφής του άρθρου 11 του ν. 2690/1999 (Α' 45). Πρόκειται για καινοτομία, απαραίτητη για την παροχή ψηφιακών υπηρεσιών με τα εχέγγυα που απαιτούν οι κείμενες διατάξεις για τη διοικητική δράση.

Όλες αυτές οι δυνατότητες που περιγράφονται παραπάνω είναι προαιρετικές, όμως σε βάθος χρόνου θα καταργηθούν ορισμένα χαρτιά με φυσικό χαρακτήρα και θα υπάρχουν μόνο τα ηλεκτρονικά έγγραφα. Ένα παράδειγμα είναι η κατάργηση του φαξ από την δημόσια διοίκηση και χρήση του ηλεκτρονικού ταχυδρομείου σε συνδυασμό με την ψηφιακή υπογραφή.

Η Ευρωπαϊκή Ένωση βαδίζει προς αυτόν τον σκοπό και είδη τρέχει πρόγραμμα «**2030 ψηφιακή πυξίδα**», προσπαθώντας να βάλει κανόνες στο διαδικτυακό τοπίο. Το ίδιο πρόγραμμα επιθυμεί να λειτουργήσει και το Ελληνικό Κράτος.

Οι συναλλαγές με το κράτος είναι κυρίως στις παρακάτω ομάδες:

1. ΟΙΚΟΝΟΜΙΚΕΣ ΕΠΙΒΑΡΥΝΣΕΙΣ ΚΑΙ ΣΥΝΑΛΛΑΓΕΣ

- Φορολογία
- Διαδικασίες είσπραξης οφειλών
- Οφειλές ΟΤΑ
- Δάνεια ΟΕΚ

2. ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ: ΟΡΟΙ ΚΑΙ ΠΕΡΙΕΧΟΜΕΝΟ

- Συγκοινωνία
- Ύδρευση

- Φοιτητική μέριμνα
- Παιδότοποι

Στις οικονομικές συναλλαγές η ψηφιοποίηση είναι σε μεγάλο βαθμό. Πλέον ο πολίτης μπορεί να συναλλάσσετε με το κράτος για να εκπληρώσει την φορολογικές του υποχρεώσεις ψηφιακά. Αυτό απαιτεί αρκετές γνώσεις πέρα από τον ψηφιακό αλφαριθμητισμό και γνώσεις φορολογίας-οικονομίας. Επίσης μπορεί να πάρει αποδεικτικά ή ότι άλλο έγγραφο χρειαστεί.

Στους δήμους εδώ και πολλά χρόνια παρατηρείται μια αναβάθμιση στις ψηφιακές υπηρεσίες. Πλέον οι δήμοι αυξάνουν τις υπηρεσίες που παρέχουν στους πολίτες ψηφιακά. Οι δημότες μπορούν πλέον να συναλλάσσονται με τον δήμο ψηφιακά είτε διεκδικώντας τα δικαιώματά τους είτε εκπληρώνοντας τις υποχρεώσεις τους διαδικτυακά.

3ο

Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025

<https://digitalstrategy.gov.gr/>

Επίσης υπάρχει και ο ψηφιακός μετασχηματισμός της Ελλάδας που δρομολογείται είδη από το 2020. Η νέα εθνική στρατηγική για τον ψηφιακό μετασχηματισμό συνοψίζεται σε επτά στόχους:

1. Η ασφαλής, γρήγορη και αξιόπιστη πρόσβαση στο διαδίκτυο για όλους
2. Η ανάπτυξη των ψηφιακών δεξιοτήτων όλων των πολιτών
3. Η στήριξη και ενίσχυση της ψηφιακής καινοτομίας
4. Η παραγωγική αξιοποίηση των δεδομένων του Δημοσίου
5. Η ένταξη των σύγχρονων τεχνολογιών σε όλους τους τομείς της οικονομίας
6. Η διευκόλυνση μετατροπής κάθε ελληνικής επιχείρησης σε ψηφιακή επιχείρηση
7. Ένα ψηφιακό κράτος, που προσφέρει καλύτερες, ψηφιακές υπηρεσίες στους πολίτες, σε όλα τα γεγονότα της ζωής τους

Μια συνοπτική παρουσίαση κάποιων ενδεικτικών παρεμβάσεων που θα υλοποιηθούν στο πλαίσιο του ψηφιακού μετασχηματισμού για την επίτευξη των επτά επί μέρους στόχων που έχουν τεθεί:

Να μπορεί κάθε πολίτης να εργαστεί με ταχύτητα, αξιοπιστία και ασφάλεια στο διαδίκτυο

1. Εξασφάλιση ευνοϊκού ρυθμιστικού και νομοθετικού πλαισίου, αναβάθμιση σταθερών δικτυακών υποδομών και διάθεση φάσματος ραδιοσυχνοτήτων για την ανάπτυξη υποδομών 5ης γενιάς (5G).
2. Ολοκλήρωση της επιθεώρησης, αποτίμησης και βελτίωσης διαδικασιών διαχείρισης και ασφάλειας πληροφοριακών συστημάτων και ψηφιακών υπηρεσιών και υποδομών με βάση τη νέα εθνική στρατηγική για την κυβερνοασφάλεια.
3. Επανασχεδιασμός ψηφιακών υπηρεσιών και ιστότοπων βάσει της αρχής του καθολικού σχεδιασμού, προκειμένου αυτά να καταστούν προσβάσιμα από όλες τις πληθυσμιακές ομάδες.

4. Αναβάθμιση εφαρμογών και συστημάτων λαμβάνοντας υπόψη την προστασία και την ιδιωτικότητα ήδη από το σχεδιασμό (security and privacy-by-design).

Να εξυπηρετήσουμε τις ανάγκες των πολιτών άμεσα και αποτελεσματικά μέσα από ένα ψηφιακό κράτος

1. Ανάπτυξη κεντρικών ψηφιακών λύσεων και παροχή νέων απλουστευμένων ψηφιακών υπηρεσιών που υλοποιούν την εξ αποστάσεως εξυπηρέτηση του πολίτη.

2. Ενιαία Εθνική Πύλη Παροχής Ψηφιακών Υπηρεσιών (gov.gr) – Υλοποίηση κεντρικού σημείου εισόδου και αναφοράς για πληροφορίες και ψηφιακές υπηρεσίες της Δημόσιας Διοίκησης. Ένταξη των πιο συχνών ή σημαντικών συναλλαγών του πολίτη με το κράτος. 3. Κέντρο Ταυτοποίησης – Υλοποίηση μοναδικού σημείου ταυτοποίησης (Single SignOn), σε όλες τις ψηφιακές υπηρεσίες που παρέχονται από τους φορείς του Δημοσίου.

4. Κέντρο Ειδοποιήσεων – Υλοποίηση κεντρικού συστήματος ειδοποιήσεων για ενημέρωση των πολιτών σχετικά με θέματα που τους αφορούν, π.χ. ενημερώσεις για την πορεία αιτημάτων τους, προσωποποιημένες ενημερώσεις προγραμμάτων προληπτικής ιατρικής, υπενθυμίσεις για υποχρεώσεις τους προς το κράτος, κ.ά.

5. Κεντρικό σύστημα συμμετοχής των πολιτών στην αξιολόγηση των προσφερόμενων υπηρεσιών του Δημοσίου και στο σχεδιασμό νέων υπηρεσιών.

6. Διασύνδεση και διαλειτουργικότητα μεταξύ των Βασικών Μητρώων μέσω του Κέντρου Διαλειτουργικότητας.

7. Υιοθέτηση πολιτικών προστασίας προσωπικών δεδομένων που ακολουθούν την αρχή της εξ ορισμού και από τη σχεδίαση συμμόρφωσης προς τις ισχύουσες προστατευτικές διατάξεις για τα προσωπικά δεδομένα.

Να βοηθήσουμε κάθε ελληνική επιχείρηση να γίνει ψηφιακή επιχείρηση

1. Κατάρτιση του ανθρώπινου δυναμικού του ιδιωτικού τομέα για την ανάπτυξη ψηφιακών δεξιοτήτων.

2. Σύστημα μέτρησης και τεκμηρίωσης του σχεδιασμού των κρατικών ενισχύσεων για τον ψηφιακό μετασχηματισμό των επιχειρήσεων.

3. Κεντρικό σύστημα ψηφιακών τιμολογίων.

4. Υποστήριξη λύσεων ηλεκτρονικού εμπορίου.

5. Ενίσχυση συστημάτων και ψηφιακών υπηρεσιών σε σχέση με τον εξαγωγικό προσανατολισμό των επιχειρήσεων.

6. Εξασφάλιση διασύνδεσης των επιχειρήσεων με το Κεντρικό και Ενιαίο Σύστημα Δημοσιονομικής Πολιτικής.

Να στηρίξουμε και να ενισχύσουμε την ψηφιακή καινοτομία

1. Εξασφάλιση του κατάλληλου περιβάλλοντος ανάπτυξης, ενίσχυσης και αποδοτικής λειτουργίας των νεοφυών επιχειρήσεων (start-ups), που δραστηριοποιούνται στον τομέα των ΤΠΕ.

2. Ανάπτυξη, συντονισμός και υποστήριξη Ψηφιακών Κέντρων Καινοτομίας (Digital Innovation Hubs), για τη δημιουργία νέων οικοσυστημάτων καινοτομίας και την επιτάχυνση του ψηφιακού μετασχηματισμού της οικονομίας.

3. Εξασφάλιση της ανοικτής διάθεσης και μέγιστης αξιοποίησης δημόσιων δεδομένων για την ανάπτυξη νέων προϊόντων, επιχειρηματικών μοντέλων και αγορών.

Να απελευθερώσουμε και να αξιοποιήσουμε την παραγωγική αξία των δεδομένων του Δημοσίου

1. Ενιαίο μοντέλο διακυβέρνησης των δεδομένων σε εθνικό επίπεδο.

2. Καθορισμός των προδιαγραφών και διαδικασιών για την ελεύθερη και ανοικτή διάθεση των δεδομένων κάθε φορέα του Δημοσίου, με συγκροτημένο και τεχνικά άρτιο τρόπο και με σεβασμό στην προστασία των προσωπικών δεδομένων.

3. Κεντρική πλατφόρμα διάθεσης και αξιοποίησης δεδομένων δημόσιου σκοπού και δεδομένων υψηλής αξίας μέσω συγκρότησης Θεματικών Αποθετηρίων Δεδομένων σε επιλεγμένους κάθετους θεματικούς άξονες.

4. Λειτουργία κέντρων διαχείρισης και ανοικτής διάθεσης δεδομένων για επιλεγμένους φορείς του δημόσιου τομέα.

5. Προγράμματα κινήτρων για την επαναχρησιμοποίηση των ανοικτών δεδομένων του Δημοσίου με σκοπό την ανάπτυξη εφαρμογών προστιθέμενης αξίας.

6. Αξιοποίηση κρίσιμων συνόλων δεδομένων και ανάπτυξη εφαρμογών Τεχνητής Νοημοσύνης, μηχανικής μάθησης, ανάλυσης μεγάλων δεδομένων και επιχειρηματικής ευφυΐας για την πάταξη λ.χ. της φοροδιαφυγής και της

εισφοροδιαφυγής, για τον έλεγχο των δημόσιων συμβάσεων, την παρακολούθηση του συστήματος εισροών και εκροών στο εμπόριο καυσίμων και κατ' επέκταση του μηχανισμού είσπραξης δημοσίων εσόδων κ.ά.

Να εντάξουμε τις σύγχρονες τεχνολογίες σε όλους τους τομείς της οικονομίας

1. Υλοποίηση εμβληματικών τομεακών έργων ανά άξονα πολιτικής με στόχο την υποστήριξη της μετάβασης υφιστάμενων συστημάτων σε νέες υποδομές και σύγχρονες αρχιτεκτονικές υλοποίησης, υποστηρίζοντας παράλληλα και νέες επιχειρησιακές διαδικασίες με οικονομικότερη συντήρηση και μεγαλύτερη ασφάλεια.

2. Υιοθέτηση σύγχρονων τεχνολογικών εργαλείων στους επί μέρους τομείς της οικονομίας, όπως εφαρμογές τηλεϊατρικής στην Υγεία, τηλεεκπαίδευσης στην Παιδεία, τηλεσυνεδριάσεων στη Δικαιοσύνη αλλά και για την εξ αποστάσεως εργασία στο Δημόσιο, αξιοποίηση δικτύου αισθητήρων για συλλογή δεδομένων στο Περιβάλλον κ.ά.

Ο ψηφιακός μετασχηματισμός της χώρας είναι μια μεγάλη πρόκληση και ένα γιγάντιο, πολύπλοκο και δύσκολο έργο. Για την υλοποίηση αυτού του έργου απαιτούνται μια στρατηγική, ένα όραμα, μια φιλοσοφία, μια μέθοδος, καθώς και η υλοποίηση σημαντικών παρεμβάσεων. Όλα τα παραπάνω είναι σημαντικό να αποτυπωθούν σε ένα ρεαλιστικό και εφικτό οδικό χάρτη, ο οποίος θα αποτελεί ένα απαραίτητο εργαλείο για ολόκληρη την εξέλιξη του ελληνικού κράτους στη δεκαετία που διανύουμε.

Ασφάλεια Ηλεκτρονικών Συναλλαγών

<https://eeke.gr/asfalia-ilektronikon-sinallagon/>

Πόσο ασφαλές είναι το Ηλεκτρονικό Εμπόριο;

Το Ηλεκτρονικό Εμπόριο, γίνεται ολοένα και πιο δημοφιλής τρόπος πραγματοποίησης συναλλαγών, λόγω της εξοικονόμησης χρόνου και ενέργειας που προσφέρει στους καταναλωτές. Παρ' όλη την εξοικείωση της κοινωνίας και ιδιαιτέρως των νεότερων ηλικιών με την τεχνολογία και τη χρήση του Internet, και παρ' όλες τις διευκολύνσεις που προσφέρει η ταχεία ανάπτυξη του Ηλεκτρονικού Εμπορίου, μεγάλο μέρος του αγοραστικού κοινού, στέκεται καχύποπτο μπροστά στη χρήση αυτού του μέσου, για την πραγματοποίηση αγορών και γενικότερα συναλλαγών. Σκεπτόμενοι λίγο πιο προσεκτικά τους κινδύνους που ελλοχεύουν, θα δικαιολογούσαμε αυτή τη στάση, καθώς το Internet σίγουρα δεν μπορεί να χαρακτηριστεί ως απόλυτα ασφαλές πεδίο συναλλαγών.

Πέραν των κινδύνων οι οποίοι αφορούν στο κατά πόσον οι όροι συναλλαγών που θέτει ένα κατάστημα ενέχουν κενά ή συγκεχυμένες πληροφορίες που ενδέχεται να αποπροσανατολίσουν, το κύριο ζήτημα που απασχολεί πολλούς καταναλωτές, είναι η παραχώρηση ευαίσθητων προσωπικών δεδομένων σε sites ηλεκτρονικών καταστημάτων των οποίων η αξιοπιστία δεν έχει ελεγχθεί.

Κάθε ηλεκτρονικό κατάστημα, θα πρέπει σύμφωνα με το νόμο, να αναφέρει λεπτομερώς την πολιτική διαχείρισης και προστασίας προσωπικών δεδομένων την οποία ακολουθεί, ώστε ο καταναλωτής να έχει τη δυνατότητα να ενημερώνεται πλήρως.

Τι είναι η κρυπτογράφηση δεδομένων;

Κρυπτογράφηση δεδομένων (cryptography), είναι η κωδικοποίηση πληροφοριών με τη βοήθεια ενός αλγόριθμου και ενός κλειδιού (key). Πρόκειται απλούστερα, για «μεταμφίεση» των πληροφοριών που ανταλλάζουν χρήστες του Διαδικτύου, ώστε να μην είναι κατανοητές σε τρίτους. Το κλειδί (key) χρησιμοποιείται ώστε να μεταβάλει το κείμενο και κατόπιν να το επαναφέρει στην αρχική του μορφή (αποκρυπτογράφηση). Η διαδικασία αυτή παρέχει ασφαλή ανταλλαγή πληροφοριών και δεδομένων και αποτρέπει τη μεσολάβηση τρίτων προσώπων με πιθανό σκοπό την υποκλοπή τους.

Ανάγκη για ασφάλεια

Όπως εύκολα γίνεται αντιληπτό, η ομαλή πραγματοποίηση συναλλαγών στο πλαίσιο του ηλεκτρονικού εμπορίου, καθιστά απαραίτητη τη χρήση πρωτοκόλλων ή άλλων μεθόδων ασφαλείας.

Τα πρωτόκολλα ασφαλείας, τα οποία θεωρούνται πλέον απαραίτητα για όλες τις συναλλαγές, χωρίζονται σε δύο κατηγορίες : Σε αυτά που λειτουργούν σε επίπεδο σύνδεσης και σε αυτά που λειτουργούν σε επίπεδο εφαρμογών.

Εκτός από τα πρωτόκολλα ασφαλείας, υπάρχουν και τα φράγματα ασφαλείας ή αλλιώς γνωστότερα ως firewalls τα οποία ελέγχουν την κίνηση δεδομένων μεταξύ ενός ιδιωτικού και ενός δημόσιου δικτύου, διατηρώντας έτσι το ιδιωτικό δίκτυο ασφαλές από εισροή επισφαλών δεδομένων. Το firewall επομένως, φιλτράρει τα δεδομένα που εισέρχονται σε ένα εσωτερικό δίκτυο και απορρίπτει κακόβουλα λογισμικά ή άλλα στοιχεία.

Πρωτόκολλα SSL και S-HTTP

Είναι τα δύο βασικά πρωτόκολλα, τα οποία εξασφαλίζουν την εμπιστευτικότητα και την ασφαλή μετάδοση δεδομένων μεταξύ χρηστών του Web.

Το πρωτόκολλο SSL (Secure Sockets Layer) το οποίο τείνει να αντικατασταθεί από το πρωτόκολλο TLS (Transport Layer Security), χρησιμοποιείται για κρυπτογράφηση δεδομένων με στόχο την ασφαλή μετάδοσή τους.

Στο πρωτόκολλο SSL υπάρχουν δύο συναλλασσόμενα μέρη, ένας server, ο οποίος μας παρέχει τις ιστοσελίδες που θέλουμε να επισκεφθούμε και ένας χρήστης, που στην προκειμένη περίπτωση είναι ο καταναλωτής που επισκέπτεται τις ιστοσελίδες και πρόκειται να αποστείλει προσωπικά του δεδομένα σε αυτές.

Ο χρήστης στέλνει αίτημα στο server για SSL επικοινωνία. Ο server από την άλλη, ο οποίος χρησιμοποιεί ψηφιακό πιστοποιητικό ασφαλείας, το αποστέλλει στο χρήστη, βεβαιώνοντάς τον, ότι η σελίδα που επισκέπτεται είναι πράγματι αυτή που δηλώνεται.

Το **HTTPS** (Hypertext Transfer Protocol Secure) χρησιμοποιείται για να δηλώσει μία ασφαλή δικτυακή σύνδεση http. Ένας σύνδεσμος (URL) που αρχίζει με το πρόθεμα https:// υποδηλώνει ότι θα χρησιμοποιηθεί κανονικά το πρωτόκολλο HTTP, αλλά η σύνδεση θα γίνει με τρόπο τέτοιο, ώστε τα δεδομένα να ανταλλάσσονται κρυπτογραφημένα.

Το HTTP κατ' ουσία, είναι ο συνδυασμός του απλού πρωτοκόλλου HTTP με το πρωτόκολλο SSL το οποίο παρέχει δυνατότητα κρυπτογράφησης δεδομένων.

Πώς αναγνωρίζω εάν μια ιστοσελίδα ηλεκτρονικού καταστήματος κάνει χρήση αυτών των πρωτοκόλλων;

Το εάν μια ιστοσελίδα κάνει χρήση αυτών των πρωτοκόλλων, είναι κάτι που ο καταναλωτής το αντιλαμβάνεται εύκολα. Προτού πραγματοποιήσουμε μια ηλεκτρονική συναλλαγή, είτε κατά την περιήγησή μας στο site του ηλεκτρονικού καταστήματος είτε στη σελίδα στην οποία πρόκειται να καταχωρίσουμε προσωπικά δεδομένα, θα πρέπει να εμφανίζεται το εικονίδιο του μικροσκοπικού λουκέτου και η ένδειξη <https://> πριν από την ηλεκτρονική διεύθυνση. Εάν εντοπίσουμε τις ενδείξεις αυτές, μπορούμε να αισθανόμαστε σχετικά ασφαλείς, όσον αφορά στη μεταφορά των προσωπικών μας δεδομένων.

ΠΡΟΣΟΧΗ! Τα πρωτόκολλα ασφαλείας, προσφέρουν ένα υψηλό επίπεδο ασφαλούς μεταφοράς δεδομένων, χωρίς όμως να κάνουμε λόγο για απόλυτη ασφάλεια και για εξαφάνιση της πιθανότητας υποκλοπής. Γι' αυτό ακριβώς το λόγο θα πρέπει σε κάθε περίπτωση, να είμαστε υποψιασμένοι και ιδιαιτέρως προσεκτικοί. Καλό είναι να αποφεύγουμε τις συναλλαγές με ηλεκτρονικό κατάστημα για την αξιοπιστία του οποίου διατηρούμε αμφιβολίες.

Τι να προσέχετε στις ηλεκτρονικές συναλλαγές

<https://www.eea.gr/arthra-eea/sistasis-gia-asfalisis-ilektronikes-sinallages/>

Η Ανεξάρτητη Αρχή “Συνήγορος του Καταναλωτή” γίνεται, όπως αναφέρεται σε σχετική ανακοίνωση, το τελευταίο διάστημα αποδέκτης πολύ μεγάλου αριθμού έγγραφων αναφορών και τηλεφωνικών παραπόνων-καταγγελιών σχετικά με προβλήματα που συναντούν οι καταναλωτές με τις διαδικτυακές αγορές τους, ιδίως προϊόντων τεχνολογίας (κινητών τηλεφώνων, τάμπλετ, φορητών υπολογιστών, κ.λπ.).

Συγκεκριμένα, οι καταναλωτές καταγγέλλουν τη μη προσήκουσα εκτέλεση των παραγγελιών τους από ηλεκτρονικά καταστήματα, τα οποία διαθέτουν προς πώληση τα προϊόντα τους σε ιδιαίτερα προνομιακές τιμές σε σχέση με τον ανταγωνισμό, προσελκύοντας μεγάλο αριθμό ενδιαφερόμενων πελατών, όπως συμβαίνει με τα αποκαλούμενα “προϊόντα-κράχτες”.

Όπως διαπιστώθηκε από την Αρχή ορισμένα από τα καταστήματα αυτά δεν παραδίδουν τα προϊόντα εντός του συμφωνημένου κατά περίπτωση χρόνου και μεταθέτουν διαρκώς τον χρόνο παράδοσης σε μελλοντικές ημερομηνίες, χωρίς, όμως, εν τέλει να τηρούν τις δεσμεύσεις τους απέναντι στους καταναλωτές και χωρίς να προβαίνουν σε επιστροφή *των χρηματικών ποσών που έχουν προεισπράξει προς ολοσχερή εξόφληση του τιμήματος των αγαθών, κατά πάγια πολιτική τους. Στις περισσότερες, δε, περιπτώσεις, οι εν λόγω

επιχειρήσεις διακόπτουν, μετά τη συναλλαγή, και κάθε επικοινωνία με τους καταναλωτές, με αποτέλεσμα να μην μπορούν να λάβουν καμία πληροφόρηση σε σχέση με την πορεία των αγορών τους ή την επιστροφή των χρημάτων τους.

Ο Συνήγορος του Καταναλωτή, στο πλαίσιο των αρμοδιοτήτων του, αναδεικνύει τις ανωτέρω αθέμιτες και παραπλανητικές εμπορικές πρακτικές και διαβιβάζει τις αναφορές που λαμβάνει στη Γενική Γραμματεία Εμπορίου και Προστασίας Καταναλωτή, για την επιβολή των προβλεπόμενων κυρώσεων. Παράλληλα, δεδομένης της αναγκαιότητας και της ποινικής διερεύνησης αυτών των υποθέσεων, προβαίνει στην υποβολή μηνυτήριων αναφορών στον αρμόδιο Εισαγγελέα Πρωτοδικών.

Περαιτέρω, η Αρχή συστήνει στους καταναλωτές για την καλύτερη προστασία τους ιδιαίτερα αυτή τη δύσκολη περίοδο:

- Να προτιμούν την πραγματοποίηση αγορών από αξιόπιστα και γνωστά ηλεκτρονικά καταστήματα. Σημαντική ένδειξη αξιοπιστίας είναι η μακρόχρονη λειτουργία των καταστημάτων στην αγορά και η ύπαρξη φυσικής έδρας τους.
- Να ελέγχουν πάντοτε τις βασικές πληροφορίες που παρέχονται για το ηλεκτρονικό κατάστημα από τον ιστότοπό του. Να αναζητούν, ειδικότερα, την επωνυμία της εταιρείας και τα πλήρη στοιχεία επικοινωνίας, συμπεριλαμβανομένης ταχυδρομικής διεύθυνσης. Η ύπαρξη μόνο ηλεκτρονικής διεύθυνσης (e-mail) και κινητού τηλεφώνου δεν αρκεί και αποτελεί, μάλιστα, ένδειξη απάτης.
- Να ελέγχουν, οπωσδήποτε, πριν από την πληρωμή ότι ο ιστότοπος παρέχει ασφαλή σύνδεση για τη μετάδοση ευαίσθητων δεδομένων, όπως στοιχείων πιστωτικών καρτών. Να βεβαιώνονται ότι το σύμβολο ασφαλούς μετάδοσης δεδομένων εμφανίζεται στο πεδίο "διεύθυνση του προγράμματος περιήγησης" – browser με τη μορφή HTTPS. Με αυτό τον τρόπο διασφαλίζουν ότι το e-shop διαθέτει SSL (Secure Sockets Layer), δηλαδή πρωτόκολλο ασφαλούς μετάδοσης ευαίσθητων δεδομένων στο διαδίκτυο, ειδικά για αγορές με πιστωτικές-χρεωστικές κάρτες και paypal.
- Να εντοπίζουν στο διαδίκτυο τυχόν σχόλια, εμπειρίες ή συστάσεις άλλων καταναλωτών που έχουν ήδη συναλλαγή με το κατάστημα. Αυτό γίνεται εύκολα, πληκτρολογώντας το όνομα της εταιρείας ή του ηλεκτρονικού καταστήματος σε μία μηχανή αναζήτησης. Να προσεγγίζουν τις συστάσεις με κριτικό μάτι, διότι μπορεί να είναι παραπλανητικές ή κατασκευασμένες.

- Τα αναγνωρισμένα ηλεκτρονικά καταστήματα έχουν στον ιστότοπό τους σήματα εμπιστοσύνης των ενώσεων ηλεκτρονικού εμπορίου και των οργανισμών που διαθέτουν πιστοποιητικά ασφαλείας και απορρήτου προσωπικών δεδομένων. Αυτό δείχνει ότι η εταιρεία είναι αξιόπιστη και ότι τηρεί τους βασικούς κανόνες στις ηλεκτρονικές συναλλαγές, οπότε ο καταναλωτής μπορεί να αγοράσει από αυτήν με ασφάλεια.
- Να αποφεύγουν την πραγματοποίηση αγορών από ηλεκτρονικά καταστήματα που απαιτούν, αποκλειστικά, την προείσπραξη του τιμήματος των αγαθών μέσω πιστωτικής/χρεωστικής κάρτας, ραγρal ή τραπεζικού εμβάσματος και δεν διαθέτουν την αντικαταβολή ή την ηλεκτρονική πληρωμή τη στιγμή της παράδοσης του προϊόντος ως εναλλακτικό τρόπο πληρωμής.
- Να μην πείθονται από τις υπερβολικά δελεαστικές τιμές των προϊόντων σε σχέση με τον ανταγωνισμό ή, εν πάση περιπτώσει, αυτό να μην είναι το μοναδικό κριτήριο για την πραγματοποίηση των αγορών τους.
- Επί σοβαρών ενδείξεων προβληματικής συναλλαγής, να προβαίνουν άμεσα σε αμφισβήτηση προς τα τραπεζικά τους ιδρύματα, εφόσον η εξόφληση των αγαθών έχει γίνει μέσω κάρτας (χρεωστικής ή πιστωτικής) και, αντίστοιχα, προς τους οργανισμούς διενέργειας ηλεκτρονικών πληρωμών (πχ. ραγρal).
- Θα πρέπει, τέλος, οι καταναλωτές να λαμβάνουν επιβεβαίωση της παραγγελίας, την οποία να φυλάσσουν μαζί με κάθε άλλο έγγραφο που σχετίζεται με αυτή. Αν χρειάζεται να επικοινωνήσουν με τον έμπορο, να προτιμούν το ηλεκτρονικό μήνυμα. Με αυτό τον τρόπο, σε περίπτωση προβλήματος, θα έχουν στη διάθεσή τους έμπρακτες αποδείξεις της επαφής-επικοινωνίας τους, καθώς και όλες τις λεπτομέρειες της συναλλαγής που έχουν συμφωνηθεί.

Για ποιόν λόγο να αγοράσω Antivirus, αφού υπάρχουν δωρεάν;

<https://techguru.gr/blog/gia-poio-logo-na-agoraso-antivirus-afou-yparchoyn-dorean/>

Ένα θέμα που απασχολεί πολλούς χρήστες υπολογιστών, με την εξάπλωση των ιών να βρίσκονται σε "έξαρση", είναι αν χρειάζεται να αγοράζουν AV (AntiVirus) ή αν μπορούν να είναι ασφαλής με ένα δωρεάν.

Όπως και να έχει είναι ένα ετήσιο κόστος, χαμηλό μεν, αλλά ίσως θα μπορούσε να αποφευχθεί;

Υπάρχει λόγος να πληρώνουμε για Antivirus; Η απάντηση είναι...και Ναι και Όχι!

Δωρεάν vs Πληρωτέο Antivirus

Οι εταιρίες AV είναι πάρα πολλές, προσφέρουν από δωρεάν απλό AV μέχρι ολόκληρη σουίτα μαζί με Firewall, εφαρμογές Antispam, system optimizers και πολλά άλλα. Έχουν διαφορές στην αποδοτικότητα, στη ταχύτητα και στη τιμή φυσικά. Δωρεάν βασική προστασία ιών προσφέρουν αρκετές εταιρίες όπως AVG, Avira, Avast, Panda αλλά και η ίδια η Microsoft με τη χρήση του Microsoft Security Essentials. Το ερώτημα είναι όμως τι διαφορές έχουν μεταξύ τους;

1. Δωρεάν AV. Το βασικότερο πλεονέκτημα των δωρεάν AV είναι φυσικά το μηδενικό κόστος του και το ότι αν δεν μας αρέσει μετά από δοκιμή...τι είχαμε τι χάσαμε! Έπειτα καταναλώνουν λίγους πόρους αφού οι δυνατότητές τους είναι λίγες. Τα πλεονεκτήματά τους όμως τελειώνουν εκεί, χωρίς να μπορούν να συναγωνιστούν τις εκδόσεις επί πληρωμή. Μιλώντας πάντα για τη πλειοψηφία των AV και συγκεκριμένες εκδόσεις, συνήθως τα δωρεάν AV προστατεύουν από βασικά malware, ορισμένα έχουν και διαφημίσεις, και λαμβάνουν updates για νέους ιούς πιο αργά από τα πληρωτέα. Φυσικά δε διαθέτουν Firewall και άλλες εξτρά λειτουργίες.

2. AntiVirus Επί Πληρωμή Τα AntiVirus επί πληρωμή διατίθενται και σε μορφή "σουίτας" όπως Internet Security, δηλαδή με εξτρά λειτουργίες όπως Firewall, Ransomware Protection, Προστασία ηλεκτρονικών πληρωμών, AntiSpam κτλ. Θα έλεγα πως το σημαντικότερο είναι το Ransomware protection το οποίο προστατεύει από ιούς που θέλουν να κρυπτογραφήσουν, δηλαδή να κλειδώσουν τα αρχεία σας ζητώντας "λύτρα". Το Firewall μπορεί να βοηθήσει για τη προστασία πάλι από Ransomware αλλά και πολλών άλλων επιθέσεων

μέσω "αδυναμιών" του συστήματος, που μπορούν να εκμεταλλευτούν επιτήδριοι στο Internet. Ορισμένες σουΐτες διαθέτουν πλήρη μενού ρυθμίσεων σε αντίθεση με τα Free, διαθέτουν online υποστήριξη από την εταιρεία, δεν έχουν διαφημίσεις και λαμβάνουν updates κάθε λίγες ώρες. Κάποιοι λένε ότι τα πληρωτέα AV διαθέτουν και καλύτερο "Engine", δηλαδή είναι καλύτερα προγραμματισμένα ώστε να αποδίδουν περισσότερο και να είναι πιο αξιόπιστα από τις δωρεάν εκδόσεις. Φυσικά αυτό δε μπορεί να αποδειχθεί με ακρίβεια. Τέλος, χρειάζεται να παρακολουθείται κάθε χρόνο πότε λήγουν, διότι αν λήξει η άδεια και δεν ανανεωθεί, σταματάει πλήρως η προστασία και μαζί τα updates για νέους ιούς.

Συνοπτικά τα συν και τα πλύν:

	Δωρεάν AntiVirus	Πληρωτέα AntiVirus
Προστασία Ransomware	Δεν διαθέτει	Διαθέτει
Εξτρά Δυνατότητες από AV	Δεν διαθέτει	Οι σουΐτες, διαθέτουν
Πλήρως Παραμετροποιήσιμα	Όχι όλα	Ναι
Διαφημίσεις	Έχουν	Δεν έχουν
Updates νέων ιών	Καθημερινά	Κάθε λίγες ώρες
Online Υποστήριξη	Όχι	Ναι
Μέριμνα ετήσιας ανανέωσης	Όχι	Ναι
Μηδενικό κόστος/Ρίσκο αγοράς	Ναι	Όχι
Ελαφρύ Λογισμικό	Ναι	Με κατάλληλη ρύθμιση, Ναι

Υπάρχει οικονομική λύση

Το κόστος ενός πληρωτέου AV δεν είναι αναγκαστικά υψηλό. Απλά φαίνεται να είναι υψηλό, στα καταστήματα!...Τι εννοούμε; Τα AV μπορούμε να τα αγοράσουμε σε 2 μορφές:

- Μορφή Retail, δηλαδή από κατάστημα με το προϊόν μέσα σε κουτί της εταιρείας που περιέχει:
 1. Ένα CD με το λογισμικό προς εγκατάσταση
 2. Την άδεια (κωδικός ενεργοποίησης) σε ένα χαρτί
 3. Ένα βιβλιαράκι με οδηγίες.

- Μορφή E-Code, δηλαδή παραλαβή μόνο του κωδικού ενεργοποίησης σε Email, καθαρά ηλεκτρονική συναλλαγή από σχετικά site.

Η πρώτη λύση είναι φυσικά ακριβότερη διότι πρόκειται για ένα ολόκληρο πακέτο προϊόντος μέσα σε ένα κατάστημα λιανικής πώλησης. Ενδεικτικά, κυμαίνεται από 30€ μέχρι 40€ ετησίως για ένα υπολογιστή. Έχει περιττά κόστη, αφού στην ουσία το κουτί και οι οδηγίες είναι περιττές, και το λογισμικό διανέμεται δωρεάν στο Internet για κατέβασμα μέσα στο σχετικό site της εκάστοτε εταιρείας σε μορφή Trial (30 ημέρες για δοκιμή) και μάλιστα στην τελευταία έκδοση, όχι σαν το CD που μπορεί να έχει παλιά. Μόλις εγκατασταθεί και μπει ο κωδικός, γίνεται πλήρης έκδοση. Οπότε μόνο ο κωδικός ηλεκτρονικά αρκεί. Είναι η οικονομικότερη λύση, κυμαίνεται μεταξύ 15€-25€ ετησίως για ένα υπολογιστή.

Το AntiVirus χρειάζεται ρύθμιση

Όταν εγκαθιστάτε ένα AV, ειδικά τα μεγαλύτερα πακέτα, χρειάζεται να παραμετροποιηθεί διότι οι προεπιλεγμένες ρυθμίσεις έχουν ενεργοποιημένες περιττές υπηρεσίες οι οποίες καταναλώνουν πόρους του συστήματος χωρίς λόγο. Επίσης καλό είναι να γίνουν ρυθμίσεις στον τρόπο ειδοποιήσεων και ευαισθησίας του AV.

Χρειάζομαι τελικά πληρωτέο AntiVirus;

Παίζει ρόλο σε ποιόν χρήστη απευθύνεται ένα AV και όχι τόσο στο μέγεθος της χρήσης που κάνει. Ένας έμπειρος χρήστης, που ξέρει πως να προφυλαχτεί στο Internet, μπορεί να του αρκεί ένα δωρεάν AV. Παρ' όλα αυτά προτείνουμε σε όλους τους χρήστες να διαθέτουν ένα πληρωτέο, έστω και βασικό πακέτο AV για σιγουριά, μιας και το κόστος των 20€/έτος δεν είναι και τόσο μεγάλο, αφού μπορεί να σας γλυτώσει από χειρότερους μπελάδες.

Συμπεράσματα

Ο ψηφιακός ανασχηματισμός του κράτους και της οικονομίας γενικότερα επιταχύνθηκε τα τελευταία χρόνια με τον covid-19. Επίσης ένα μεγάλο μέρος του πληθυσμού εξοικειώθηκε με τις νέες τεχνολογίες και αυτό ανέβασε σε πληθυσμό τους δυνητικούς πελάτες των ψηφιακών επιχειρήσεων με αποτέλεσμα την περεταίρω ανάπτυξή τους. Οι ηλεκτρονικές συναλλαγές όμως κρύβουν κινδύνους που απαιτούν προσοχή και γνώση, οι πελάτες οφείλουν να προσέχουν στις συναλλαγές. Επιπλέον σημαντικό είναι για όλους που κάνουν ηλεκτρονικές συναλλαγές να χρησιμοποιούν antivirus.

Το κράτος με όλες τις δομές τους ανέπτυξε ψηφιακές διαδικασίες για συναλλαγές με τους πολίτες πιο γρήγορα σε σχέση με το προγραμματιζόμενο, επίσης λόγω covid-19, συνεχίζει να το κάνει με τον ίδιο ρυθμό. Αυτό έδωσε την δυνατότητα στους πολίτες να αλληλοεπιδρούν μαζί του σε μεγαλύτερο βαθμό, ο οποίος θα αυξάνεται.

Πληροφορίες για τους νόμους που ισχύουν πέρα από τις κρατικές ιστοσελίδες υπάρχουν στις ιστοσελίδες για τους καταναλωτές όπως και στην ιστοσελίδα της ευρωπαϊκής ένωσης, πολύ αναλυτικά για τα δικαιώματα των καταναλωτών και των πνευματικών δικαιωμάτων.