ΕΝΟΤΗΤΑ 6 – ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

ΥΠΟΕΝΟΤΗΤΑ 6.2
Καλές πρακτικές και ασφάλεια ηλεκτρονικών πληρωμών

ΕΙΣΑΓΩΓΗ ΜΑΘΗΜΑΤΟΣ	Με την αύξηση των ηλεκτρονικών αγορών και των ψηφιακών συναλλαγών, είναι ζωτικής σημασίας να διατηρείτε τις ηλεκτρονικές σας πληρωμές ασφαλείς για την προστασία των οικονομικών σας πληροφοριών. Η ασφάλεια των ηλεκτρονικών πληρωμών περιλαμβάνει μέτρα για τη διαφύλαξη των προσωπικών και οικονομικών σας στοιχείων όταν πραγματοποιείτε αγορές ή συναλλαγές στο διαδίκτυο. Κατανοώντας τους κινδύνους και λαμβάνοντας προφυλάξεις, μπορείτε να μειώσετε τις πιθανότητες απάτης ή κλοπής ταυτότητας. Η ασφάλεια των ηλεκτρονικών πληρωμών περιλαμβάνει μέτρα για την προστασία των προσωπικών και οικονομικών σας στοιχείων από το να πέσουν σε λάθος χέρια. Μια ουσιαστική πτυχή είναι η ενημέρωση σχετικά με το "Ψάρεμα" (phishing). Σε αυτό το μάθημα, θα μάθετε πώς να είστε ασφαλείς όταν πραγματοποιείτε ηλεκτρονικές πληρωμές χάρη σε έναν κατάλογο καλών πρακτικών και συμβουλών σχετικά με την ασφάλεια στο διαδίκτυο όταν υπάρχουν οικονομικές πτυχές.
ΕΛΕΓΧΟΣ ΠΡΟΗΓΟΥΜΕΝΩΝ ΕΡΓΑΣΙΩΝ	Κατά τη διάρκεια του παιχνιδιού ρόλων, οι συμμετέχοντες θα αναλάβουν διαφορετικούς ρόλους, σύμφωνα με την έρευνα που έχουν πραγματοποιήσει. Αφήστε χώρο για ελεύθερη έκφραση και πλούσια αλληλεπίδραση μεταξύ των μαθητών, παρεμβαίνετε μόνο όταν είναι απαραίτητο. Αυτή η προσέγγιση τους επιτρέπει να εξερευνήσουν πραγματικές

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	καταστάσεις και να αναπτύξουν πρακτικές δεξιότητες για την ασφαλή πλοήγηση στις ηλεκτρονικές πληρωμές.
ΕΙΣΑΓΩΓΗ	Η καλύτερη μέθοδος για την ασφάλεια των ηλεκτρονικών πληρωμών είναι να ενημερώνετε τακτικά το λογισμικό σας. Αυτό περιλαμβάνει το λειτουργικό σας σύστημα, το πρόγραμμα περιήγησης στο διαδίκτυο και οποιοδήποτε λογισμικό ασφαλείας χρησιμοποιείτε. Οι ενημερώσεις συχνά περιλαμβάνουν διορθώσεις για γνωστά ζητήματα ασφαλείας, γεγονός που συμβάλλει στην προστασία των προσωπικών και οικονομικών σας πληροφοριών από απειλές στον κυβερνοχώρο. Ενεργοποιήστε τις αυτόματες ενημερώσεις όποτε είναι δυνατόν, για να διασφαλίσετε ότι χρησιμοποιείτε τις πιο ασφαλείς εκδόσεις λογισμικού. Η χρήση ασφαλών ιστότοπων είναι ζωτικής σημασίας όταν πραγματοποιείτε ηλεκτρονικές συναλλαγές. Αναζητήστε το "https" στη διεύθυνση URL, που υποδηλώνει μια ασφαλή σύνδεση που κρυπτογραφεί τα δεδομένα σας. Αποφύγετε την εισαγωγή ευαίσθητων πληροφοριών σε ιστότοπους χωρίς αυτή την ασφαλή σύνδεση και να είστε προσεκτικοί σε ιστότοπους που ζητούν περιττά προσωπικά στοιχεία. Είναι προτιμότερο να είστε προσεκτικοί όταν έχετε αμφιβολίες για τη νομιμότητα ενός ιστότοπου. Η παρακολούθηση της δραστηριότητας του λογαριασμού σας είναι απαραίτητη για την ασφάλεια των ηλεκτρονικών πληρωμών. Ελέγχετε τακτικά τις καταστάσεις του λογαριασμού σας και το ιστορικό των συναλλαγών σας για να εντοπίζετε τυχόν μη εξουσιοδοτημένη ή ύποπτη δραστηριότητα. Ελέγξτε τον λογαριασμό σας τουλάχιστον εβδομαδιαίως και ρυθμίστε ειδοποιήσεις για μεγάλες ή ασυνήθιστες συναλλαγές για να ενημερώνεστε σε πραγματικό χρόνο. Εάν παρατηρήσετε μη εξουσιοδοτημένες ή ύποπτες συναλλαγές, αναφέρετε τις

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	αμέσως στο χρηματοπιστωτικό σας ίδρυμα. Οι περισσότερες τράπεζες και εταιρείες πιστωτικών καρτών διαθέτουν τμήματα απάτης για τη διερεύνηση και επίλυση τέτοιων ζητημάτων. Συνιστάται η τήρηση αρχείων της επικοινωνίας σας με το χρηματοπιστωτικό σας ίδρυμα σχετικά με ύποπτες συναλλαγές για μελλοντική αναφορά. Επιπλέον, λάβετε προληπτικά μέτρα για την προστασία των πληροφοριών των ηλεκτρονικών σας πληρωμών. Χρησιμοποιήστε ασφαλείς και μοναδικούς κωδικούς πρόσβασης για τους λογαριασμούς σας, ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων και αποφύγετε τη χρήση δημόσιων δικτύων Wi-Fi για ηλεκτρονικές πληρωμές.
ΓΕΝΙΚΗ ΘΕΩΡΙΑ	Όσον αφορά την ασφάλεια, τα συστήματα ηλεκτρονικών πληρωμών διαθέτουν προηγμένα μέτρα για την προστασία των ευαίσθητων πληροφοριών. Η τεχνολογία κρυπτογράφησης διασφαλίζει τη μετάδοση δεδομένων και ο έλεγχος ταυτότητας δύο παραγόντων επαληθεύει την ταυτότητα των χρηστών, ελαχιστοποιώντας τους κινδύνους απάτης. Παρά τις εγγυήσεις αυτές, οι χρήστες θα πρέπει ακόμη να λαμβάνουν προφυλάξεις, όπως η χρήση ισχυρών κωδικών πρόσβασης, η αποφυγή δημόσιου Wi-Fi για συναλλαγές και η τακτική παρακολούθηση των λογαριασμών για την αποτροπή απειλών στον κυβερνοχώρο. Οι ηλεκτρονικές πληρωμές προσφέρουν πολλά πλεονεκτήματα στους καταναλωτές, όπως ευκολία, ευελιξία και ασφάλεια. Η πραγματοποίηση πληρωμών μέσω διαδικτύου είναι βολική, καθώς οι πελάτες μπορούν να το κάνουν οποτεδήποτε και οπουδήποτε με σύνδεση στο διαδίκτυο, εξαλείφοντας την ανάγκη επίσκεψης σε φυσικό κατάστημα ή τράπεζα. Επιπλέον, οι ηλεκτρονικές πληρωμές παρέχουν ευελιξία,

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	καθώς προσφέρουν διάφορες επιλογές πληρωμής, όπως πιστωτικές κάρτες, χρεωστικές κάρτες και ψηφιακά πορτοφόλια. Οι απάτες ηλεκτρονικού "ψαρέματος" (phishing scams) συχνά περιλαμβάνουν παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα που υποδύονται αξιόπιστες οντότητες για να σας εξαπατήσουν ώστε να αποκαλύψετε ευαίσθητες πληροφορίες. Για να αποφύγετε να πέσετε θύμα, να είστε προσεκτικοί στα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου και ποτέ μην κάνετε κλικ σε ύποπτους συνδέσμους ή μην παρέχετε προσωπικές πληροφορίες. Καλές πρακτικές για την ασφάλεια των ηλεκτρονικών πληρωμών μπορεί να είναι: 1) Χρησιμοποιήστε ένα Εικονικό Ιδιωτικό Δίκτυο (VPN): Εξετάστε το ενδεχόμενο χρήσης ενός VPN όταν πραγματοποιείτε online πληρωμές, ειδικά όταν χρησιμοποιείτε δημόσια δίκτυα Wi-Fi. Ένα VPN κρυπτογραφεί τη σύνδεσή σας στο διαδίκτυο, παρέχοντας ένα πρόσθετο επίπεδο ασφάλειας και ιδιωτικότητας. 2) Ελέγχετε τακτικά τις ρυθμίσεις απορρήτου: Αφιερώστε χρόνο για να επανεξετάζετε και να ενημερώνετε τακτικά τις ρυθμίσεις απορρήτου στους λογαριασμούς και τις συσκευές σας. Περιορίστε την ποσότητα των προσωπικών πληροφοριών που μοιράζεστε στο διαδίκτυο για να ελαχιστοποιήσετε τον κίνδυνο κλοπής ταυτότητας και μη εξουσιοδοτημένης πρόσβασης στους λογαριασμούς σας. 3) Να είστε προσεκτικοί με τις απάτες μέσω ηλεκτρονικού ταχυδρομείου και τηλεφώνου: Να είστε επιφυλακτικοί απέναντι σε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνήματα που ζητούν προσωπικές ή οικονομικές πληροφορίες,

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	ακόμη και αν φαίνεται να προέρχονται από νόμιμες πηγές. Αποφεύγετε να κάνετε κλικ σε συνδέσμους ή να κατεβάζετε συνημμένα αρχεία από άγνωστες ή ύποπτες πηγές. 4) Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων: Όποτε είναι δυνατόν, ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) για τους διαδικτυακούς σας λογαριασμούς. Ο MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας απαιτώντας πρόσθετη επαλήθευση πέραν του κωδικού πρόσβασης, όπως έναν κωδικό μιας χρήσης που αποστέλλεται στο τηλέφωνό σας. 5) Κρατήστε αντίγραφα ασφαλείας των σημαντικών δεδομένων: Δημιουργείτε τακτικά αντίγραφα ασφαλείας σημαντικών εγγράφων και δεδομένων που είναι αποθηκευμένα στις συσκευές σας, όπως οικονομικά αρχεία και αποδείξεις συναλλαγών. Σε περίπτωση παραβίασης της ασφάλειας ή απώλειας δεδομένων, η ύπαρξη αντιγράφων ασφαλείας διασφαλίζει ότι μπορείτε να εξακολουθείτε να έχετε πρόσβαση σε κρίσιμες πληροφορίες.
Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΙΤΑΛΙΑΣ	Συνοψίσαμε και μεταφράσαμε μια πρόσφατη μελέτη της εφημερίδας "Il Sole 24 Ore" (https://www.ilsole24ore.com/art/la-sicurezza-informatica-passa-nuovi-modelli-relazione-i-cittadini-clienti-AF3AldXC), η οποία παρέχει ορισμένα πολύ ενδιαφέροντα στοιχεία σχετικά με τις τελευταίες εξελίξεις σε ιταλικό επίπεδο στο θέμα των ηλεκτρονικών πληρωμών: Στην Ευρώπη και στην Ιταλία, υπάρχει επείγουσα ανάγκη να γεφυρωθεί γρήγορα και αποτελεσματικά το χάσμα στην άμυνα της κυβερνοασφάλειας τόσο για το σύστημα της χώρας όσο και για μεμονωμένα στρατηγικά περιουσιακά στοιχεία, ξεκινώντας από τις μικρές και μεγάλες

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	επιχειρήσεις. Τόσο η Κεντρική Δημόσια Διοίκηση (CPA) όσο και η Τοπική Δημόσια Διοίκηση (LPA) χειρίζονται καθημερινά ευαίσθητες πληροφορίες και παρέχουν κρίσιμες και συχνά απαραίτητες υπηρεσίες. Αυτή η στροφή προς την ενίσχυση της ασφάλειας στον κυβερνοχώρο υποστηρίζεται από πρόσφατους κανονισμούς, τόσο σε ευρωπαϊκό (κανονισμός της ΕΕ 7 Ιαν. 2023/2841) όσο και σε εθνικό επίπεδο (σχέδιο νόμου για την ασφάλεια στον κυβερνοχώρο που εγκρίθηκε από το Υπουργικό Συμβούλιο στις 25 Ιανουαρίου). Οι κανονισμοί αυτοί αποσκοπούν στην επιτάχυνση και την προώθηση της υιοθέτησης συγκεκριμένων μέτρων για τον μετριασμό του κινδύνου στον κυβερνοχώρο που αντιμετωπίζουν τόσο οι δημόσιοι όσο και οι ιδιωτικοί φορείς. Τα τελευταία χρόνια, οι κυβερνοεπιθέσεις έχουν αυξηθεί σε αριθμό και αποτελεσματικότητα, επηρεάζοντας τις λειτουργίες εταιρειών και δημόσιων διοικήσεων που παρέχουν στρατηγικές υπηρεσίες και διαχειρίζονται ευαίσθητα δεδομένα. Οι οικονομικές συνέπειες και οι αυξημένες διακοπές των υπηρεσιών επηρεάζουν τις κοινότητες, τους πολίτες-χρήστες και τους πελάτες. Οι βασικοί θεσμοί δεν μπορούν να μείνουν εκτεθειμένοι σε τέτοιους κινδύνους, ιδίως αν ληφθεί υπόψη η πολιτική, οικονομική και κοινωνική αστάθεια που προκύπτει από τα σενάρια διεθνών συγκρούσεων. Η έκδοση του νέου ευρωπαϊκού κανονισμού αποσκοπεί στην επιτάχυνση της προσαρμογής και της αντιμετώπισης των κινδύνων στον κυβερνοχώρο, θεσπίζοντας μέτρα για την αύξηση των επιπέδων ασφάλειας στον κυβερνοχώρο εντός των θεσμικών οργάνων και των φορέων της ΕΕ. Ο κανονισμός ορίζει μέτρα για τη θέσπιση εσωτερικού πλαισίου διαχείρισης κινδύνων, διακυβέρνησης και ελέγχου για κάθε φορέα

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	και θεσπίζει μια νέα διοργανική επιτροπή για την ασφάλεια στον κυβερνοχώρο (IICB), η οποία έχει ως αποστολή την παρακολούθηση και την υποστήριξη της ορθής εφαρμογής των νέων κανόνων. Σε εθνικό επίπεδο, το σχέδιο νόμου για την ασφάλεια στον κυβερνοχώρο επεκτείνει το εύρος των ζητημάτων που απαιτείται για την αναφορά ενός σχετικού συμβάντος. Αναθέτει στις οντότητες να αναπτύξουν μια εσωτερική δομή που θα είναι υπεύθυνη για τον καθορισμό στρατηγικών για τη διαχείριση των κινδύνων κυβερνοασφάλειας και την εφαρμογή σχεδίων δράσης και παρακολούθησης των κινδύνων. Το σχέδιο νόμου εισάγει επίσης μια νέα υπόθεση κρατικής ευθύνης και διοικητικών κυρώσεων σε περιπτώσεις μη συμμόρφωσης με τις καθιερωμένες υποχρεώσεις. Υπάρχει αναμφίβολα αυξημένη ευαισθησία σε αυτά τα ζητήματα στην αγορά κυβερνοασφάλειας. Οι δημόσιοι και ιδιωτικοί οργανισμοί αρχίζουν να προσεγγίζουν τον ψηφιακό μετασχηματισμό με έμφαση στην "ασφαλή ψηφιακή καινοτομία", δίνοντας μεγαλύτερη σημασία στις πτυχές της κυβερνοασφάλειας μέσω προηγμένων εργαλείων για τον εντοπισμό παραβιάσεων, τον καθορισμό αποτελεσματικότερων στρατηγικών αντιμετώπισης και την παροχή καινοτόμων υπηρεσιών άμυνας για στρατηγικά περιουσιακά στοιχεία. Τα πλεονεκτήματα είναι αντικειμενικά σημαντικά, διότι το κόστος φήμης, οι διακοπές υπηρεσιών και η απώλεια πληροφοριών είναι υπαρκτά και κανένας συνετός δημόσιος υπάλληλος δεν μπορεί να τα αγνοήσει ή να απέχει από τη λήψη μέτρων για την αντιμετώπισή τους. Ο μετασχηματισμός αυτός συνεπάγεται πλήρη επανεξέταση των επιχειρησιακών

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	διαδικασιών σε μια προοπτική βαθιάς καινοτομίας, η οποία ενεργοποιείται από νέα μοντέλα σχέσεων με τους χρήστες και παροχής υπηρεσιών. Η καινοτομία επιφέρει θετικό μετασχηματισμό όχι μόνο για το ίδιο το ίδρυμα αλλά και για τους πολίτες και τους ιδιώτες που επωφελούνται από τις υπηρεσίες. Είναι ευθύνη των φορέων του κλάδου να καταστήσουν την πρόσβαση σε προηγμένες υπηρεσίες κυβερνοασφάλειας πιο "δημοκρατική". Η πρόκληση είναι να γίνουν οι υπηρεσίες αυτές όλο και πιο απλές, εύκολες στη διαμόρφωση και τη διαχείριση και προσιτές σε μικρούς και μεσαίους οργανισμούς χωρίς να θυσιάζεται η αποτελεσματικότητα.
ΠΑΡΑΔΕΙΓΜΑΤΑ	1. Η Μαρία, μία ηλικιωμένη, ψωνίζει τακτικά στο διαδίκτυο είδη παντοπωλείου. Πριν κάνει οποιεσδήποτε αγορές, ελέγχει πάντα για το σύμβολο λουκέτου στη γραμμή διευθύνσεων του προγράμματος περιήγησης και διασφαλίζει ότι η διεύθυνση URL του ιστότοπου ξεκινά με "https://" για να επιβεβαιώσει ότι ο ιστότοπος είναι ασφαλής. Ακολουθώντας αυτή την πρακτική, η Μαρία προστατεύει τα προσωπικά και οικονομικά της στοιχεία από πιθανές απειλές στον κυβερνοχώρο. 2.Ο Τζιοβάνι, ένας άλλος ηλικιωμένος, ελέγχει συχνά τις κινήσεις του τραπεζικού του λογαριασμού και τις συναλλαγές πιστωτικών καρτών μέσω διαδικτύου. Πρόσφατα, παρατήρησε μια ύποπτη συναλλαγή στην κίνηση της πιστωτικής του κάρτας. Χωρίς καθυστέρηση, ο Τζιοβάνι ανέφερε τη μη εξουσιοδοτημένη χρέωση στην τράπεζά του, η οποία διερεύνησε αμέσως το ζήτημα και επέστρεψε το ποσό. Η επαγρύπνηση του Τζιοβάνι όσον αφορά την παρακολούθηση της δραστηριότητας του λογαριασμού του τον βοήθησε να

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	εντοπίσει και να αντιμετωπίσει γρήγορα πιθανή δόλια δραστηριότητα. 3. Η Σάρα, συνταξιούχος επαγγελματίας, απολαμβάνει να χρησιμοποιεί διάφορες διαδικτυακές υπηρεσίες για επικοινωνία και ψυχαγωγία. Για να διασφαλίσει την ασφάλεια των λογαριασμών της, η Σάρα ακολουθεί τη συμβουλή της δημιουργίας ισχυρών και μοναδικών κωδικών πρόσβασης για κάθε έναν από τους διαδικτυακούς λογαριασμούς της. Χρησιμοποιεί ένα συνδυασμό γραμμάτων, αριθμών και ειδικών χαρακτήρων και αποφεύγει να χρησιμοποιεί πληροφορίες που κάποιος μπορεί να μαντέψει εύκολα, όπως το όνομα ή την ημερομηνία γέννησής της. Διατηρώντας ισχυρούς κωδικούς πρόσβασης, η Σάρα μειώνει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης στους διαδικτυακούς λογαριασμούς της.
ΠΡΑΚΤΙΚΗ ΑΣΚΗΣΗ	Ποια είναι μια από τις καλές πρακτικές για τη διασφάλιση της ασφάλειας των ηλεκτρονικών πληρωμών; α. Κοινή χρήση κωδικών πρόσβασης με φίλους β. Χρήση δημόσιου Wi-Fi για συναλλαγές γ. Έλεγχος για το σύμβολο του λουκέτου στη γραμμή διευθύνσεων του προγράμματος περιήγησης δ. Κλικ σε ύποπτους συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου Ποιο από τα παρακάτω αποτελεί ασφαλή μέθοδο πληρωμής για ηλεκτρονικές συναλλαγές; α. Αποστολή μετρητών σε φάκελο β. Χρήση πιστωτικής κάρτας με τεχνολογία κρυπτογράφησης γ. Κοινοποίηση του αριθμού κοινωνικής ασφάλισής σας σε άγνωστους ιστότοπους δ. Κοινοποίηση του αριθμού PIN σας με διαδικτυακούς εμπόρους λιανικής πώλησης

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	Πόσο συχνά πρέπει να παρακολουθείτε τις οικονομικές σας καταθέσεις και τις πιστωτικές σας αναφορές για ύποπτη δραστηριότητα; α. Ποτέ β. Μία φορά το χρόνο γ. Τουλάχιστον μία φορά το μήνα δ. Μόνο όταν λαμβάνετε ειδοποίηση από την τράπεζά σας Τι πρέπει να κάνετε εάν παρατηρήσετε μη εξουσιοδοτημένες συναλλαγές στο λογαριασμό σας; α. Να τις αγνοήσετε, καθώς πιθανότατα θα επιλυθούν από μόνες τους β. Να τις αναφέρετε αμέσως στο χρηματοπιστωτικό σας ίδρυμα γ. Περιμένετε τον επόμενο λογαριασμό για να δείτε αν θα ξανασυμβούν δ. Μοιραστείτε τις πληροφορίες στα μέσα κοινωνικής δικτύωσης για να προειδοποιήσετε τους άλλους Ποιο από τα παρακάτω ΔΕΝ αποτελεί συνιστώμενη πρακτική για την ασφάλεια των ηλεκτρονικών πληρωμών; α. Χρήση ισχυρών και μοναδικών κωδικών πρόσβασης για κάθε διαδικτυακό λογαριασμό β. Αποφυγή δημόσιων δικτύων Wi-Fi για συναλλαγές γ. Κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς δ. Έλεγχος για ασφαλείς συνδέσεις σε δικτυακούς τόπους πριν από την εισαγωγή ευαίσθητων πληροφοριών *Σωστές απαντήσεις* *1 – Γ* *2 – Β* *3 – Γ* *4 – Β* *5 – Γ*

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

ΘΕΜΑ ΠΡΟΣ ΣΥΖΗΤΗΣΗ	Σε μια εποχή αυξανόμενης ψηφιοποίησης, πιστεύετε ότι οι παραδοσιακές μέθοδοι πληρωμής, όπως τα μετρητά ή οι επιταγές, εξακολουθούν να έχουν σημασία ή καθίστανται παρωχημένες υπέρ των ηλεκτρονικών πληρωμών; Γιατί? «Πώς μπορούμε να επιτύχουμε μια ισορροπία μεταξύ της αποδοχής της ευκολίας των ηλεκτρονικών πληρωμών και της διασφάλισης της ασφάλειας των οικονομικών μας πληροφοριών; Ποια μέτρα θεωρείτε απαραίτητα για την επίτευξη αυτής της ισορροπίας;
ΣΧΟΛΙΑ	Στόχος της παρούσας εργασίας είναι να δώσει στους συμμετέχοντες τις γνώσεις και τις δεξιότητες ώστε να ενισχύσουν την ασφάλεια των ηλεκτρονικών πληρωμών τους μέσω της ανάπτυξης και εφαρμογής ενός εξατομικευμένου καταλόγου ελέγχου ασφάλειας ηλεκτρονικών πληρωμών. Σε αυτή την εργασία, οι συμμετέχοντες θα αναπτύξουν έναν ολοκληρωμένο κατάλογο ελέγχου ασφάλειας ηλεκτρονικών πληρωμών, εστιάζοντας σε βασικά μέτρα ασφαλείας για τις ηλεκτρονικές συναλλαγές, όπως η ασφάλεια του ιστότοπου, η διαχείριση κωδικών πρόσβασης και οι ασφαλείς μέθοδοι πληρωμής. Στη συνέχεια, θα επανεξετάσουν τις τρέχουσες πρακτικές τους για τις ηλεκτρονικές πληρωμές, συμπεριλαμβανομένων των ιστότοπων που χρησιμοποιούν, των μεθόδων πληρωμής που χρησιμοποιούν και των στρατηγικών διαχείρισης κωδικών πρόσβασης. Αφού συγκρίνουν τις πρακτικές τους με τα στοιχεία του καταλόγου ελέγχου, θα εντοπίσουν τυχόν κενά ή περιοχές για βελτίωση στην ασφάλεια των ηλεκτρονικών πληρωμών τους. Με βάση αυτή την αξιολόγηση, οι συμμετέχοντες θα κάνουν τις απαραίτητες προσαρμογές στις πρακτικές τους, εφαρμόζοντας πρόσθετα μέτρα ασφαλείας ή αλλάζοντας τα υπάρχοντα για να ενισχύσουν την ασφάλεια. Τέλος, θα

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393

	γράψουν έναν σύντομο απολογισμό, όπου θα συζητούν τυχόν προκλήσεις που αντιμετώπισαν κατά τη φάση της αξιολόγησης και της προσαρμογής και θα αναλογίζονται τη σημασία της ασφάλειας των ηλεκτρονικών πληρωμών για την προσωπική οικονομική ασφάλεια.

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή αυτής της έκδοσης δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει τις απόψεις μόνο για τους συγγραφείς, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.
Βασική δράση 2 – Συμπράξεις μικρής κλίμακας στην εκπαίδευση ενηλίκων
Αριθμός έργου: 2022-2-EL01-KA210-ADU-000093393