ΕΝΟΤΗΤΑ 3
Τραπεζικές Εργασίες και Ψηφιακές Δεξιότητες

ΥΠΟΕΝΟΤΗΤΑ 3.2: Παραμένοντας ασφαλείς στο διαδίκτυο: πρακτικές ασφάλειας για την ψηφιακή τραπεζική

ΕΙΣΑΓΩΓΉ ΜΑΘΉΜΑΤΟΣ	Σε αυτή την ενότητα, παρουσιάζουμε το κρίσιμο θέμα της διαδικτυακής ασφάλειας για την ψηφιακή τραπεζική. Τονίζουμε τη σημασία της κατανόησης των μέτρων ασφαλείας για την προστασία των προσωπικών και οικονομικών πληροφοριών κατά τη διεξαγωγή συναλλαγών στο διαδίκτυο. Αυτή η γνώση εξασφαλίζει ασφαλέστερες και πιο σίγουρες αλληλεπιδράσεις με τις πλατφόρμες ψηφιακής τραπεζικής.
ΕΛΕΓΧΟΣ ΠΡΟΗΓΟΥΜΕΝΩΝ ΕΡΓΑΣΙΩΝ	Δ / Υ
ΕΙΣΑΓΩΓΗ ΣΤΟ ΘΕΜΑ	Η ενότητα 4.2 επικεντρώνεται στον εξοπλισμό σας με βασικές δεξιότητες για να παραμείνετε ασφαλείς ενώ κάνετε τραπεζικές συναλλαγές στο διαδίκτυο. Καθώς όλο και περισσότερες χρηματοπιστωτικές υπηρεσίες μετακινούνται σε ψηφιακές πλατφόρμες, η γνώση του τρόπου αναγνώρισης και αποφυγής πιθανών κινδύνων, όπως οι απάτες ηλεκτρονικού ψαρέματος, είναι ζωτικής σημασίας. Αυτή η μονάδα θα σας δώσει τη δυνατότητα να πλοηγηθείτε στις ηλεκτρονικές τραπεζικές συναλλαγές με ασφάλεια και σιγουριά.
ΓΕΝΙΚΗ ΘΕΩΡΙΑ	Η κατανόηση και η εφαρμογή μέτρων ασφάλειας στο διαδίκτυο είναι ζωτικής σημασίας για την ασφαλή ψηφιακή τραπεζική και τη συνολική χρήση του διαδικτύου. Με αυτόν τον τρόπο, τα άτομα μπορούν να ενισχύσουν σημαντικά τη στάση τους στον κυβερνοχώρο και να προστατευθούν από διαδικτυακές απειλές. Αυτές οι πρακτικές προωθούν μια ασφαλή και σίγουρη διαδικτυακή εμπειρία, ζωτικής σημασίας για τη διατήρηση του ελέγχου των προσωπικών οικονομικών και των ψηφιακών αλληλεπιδράσεων. Σημασία ισχυρών κωδικών πρόσβασης και ελέγχου ταυτότητας δύο παραγόντων Ισχυροί κωδικοί πρόσβασης:

Co-funded by the European Union

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

	• Ορισμός: Οι ισχυροί κωδικοί πρόσβασης είναι περίπλοκοι και δύσκολο να μαντέψουν οι άλλοι. Συνήθως περιλαμβάνουν ένα συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και ειδικών χαρακτήρων. • Σημαντικό: Οι ισχυροί κωδικοί πρόσβασης είναι η πρώτη γραμμή άμυνας κατά της μη εξουσιοδοτημένης πρόσβασης στους λογαριασμούς σας. Καθιστούν πιο δύσκολο για τους χάκερ να σπάσουν ή να μαντέψουν τον κωδικό πρόσβασής σας χρησιμοποιώντας αυτοματοποιημένα εργαλεία. Έλεγχος ταυτότητας δύο παραγόντων (2FA): • Ορισμός: Το 2FA προσθέτει ένα επιπλέον επίπεδο ασφάλειας απαιτώντας όχι μόνο έναν κωδικό πρόσβασης αλλά και μια δεύτερη πληροφορία, συνήθως έναν κωδικό που αποστέλλεται στο τηλέφωνό σας ή δημιουργείται από μια εφαρμογή. • Σπουδαιότητα: Ακόμα κι αν κάποιος καταφέρει να αποκτήσει τον κωδικό πρόσβασής σας, θα χρειαστεί τον δεύτερο παράγοντα (π.χ. το τηλέφωνό σας) για να αποκτήσει πρόσβαση στον λογαριασμό σας. Αυτό ενισχύει σημαντικά την ασφάλεια και μειώνει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης. Αναγνώριση προσπαθειών ηλεκτρονικού ψαρέματος (phishing) και άλλων συνηθισμένων απατών Απόπειρες ηλεκτρονικού ψαρέματος: • Ορισμός: Το ηλεκτρονικό ψάρεμα (phishing) είναι μια δόλια προσπάθεια απόκτησης ευαίσθητων πληροφοριών (όπως κωδικοί πρόσβασης, ονόματα χρήστη, στοιχεία πιστωτικών καρτών) προσποιούμενοι ότι είναι αξιόπιστη οντότητα σε μια ηλεκτρονική επικοινωνία. • Αναγνώριση σημείων: Τα μηνύματα ηλεκτρονικού "ψαρέματος" συχνά ζητούν ευαίσθητες πληροφορίες, χρησιμοποιούν γενικούς χαιρετισμούς, περιέχουν ορθογραφικά ή γραμματικά λάθη ή έχουν ύποπτους συνδέσμους ή συνημμένα. • Σπουδαιότητα: Η δυνατότητα αναγνώρισης προσπαθειών ηλεκτρονικού ψαρέματος (phishing) συμβάλλει στην αποτροπή του να πέσετε θύμα κλοπής ταυτότητας, οικονομικής απάτης και άλλων εγκλημάτων στον κυβερνοχώρο.

Co-funded by the European Union

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

	Προστασία προσωπικών πληροφοριών στο διαδίκτυο • Προσωπικές πληροφορίες: Αυτό περιλαμβάνει λεπτομέρειες όπως το πλήρες όνομά σας, τη διεύθυνση, την ημερομηνία γέννησης, τον αριθμό κοινωνικής ασφάλισης και τυχόν οικονομικές πληροφορίες. • Βέλτιστες πρακτικές: ○ Παρέχετε προσωπικές πληροφορίες μόνο σε ασφαλείς ιστότοπους (αναζητήστε HTTPS στη διεύθυνση URL). ○ Να είστε προσεκτικοί σχετικά με την κοινή χρήση προσωπικών στοιχείων στα μέσα κοινωνικής δικτύωσης και σε άλλες διαδικτυακές πλατφόρμες. ○ Αποφύγετε να απαντάτε σε αυτόκλητα αιτήματα για προσωπικές πληροφορίες. • Σπουδαιότητα: Η προστασία των προσωπικών πληροφοριών μειώνει τον κίνδυνο κλοπής ταυτότητας, απάτης και κατάχρησης των δεδομένων σας από κακόβουλους παράγοντες. Κατανόηση του ρόλου του λογισμικού ασφαλείας και των ενημερώσεων Λογισμικό ασφαλείας: • Ορισμός: Το λογισμικό ασφαλείας περιλαμβάνει προγράμματα προστασίας από ιούς, τείχη προστασίας και εργαλεία προστασίας από λογισμικό κακόβουλης λειτουργίας που έχουν σχεδιαστεί για την προστασία των συσκευών σας από κακόβουλο λογισμικό και απειλές στον κυβερνοχώρο. • Ρόλος: Το λογισμικό ασφαλείας σαρώνει και αφαιρεί ιούς, κακόβουλο λογισμικό και άλλες απειλές, παρέχοντας ένα επίπεδο άμυνας έναντι κυβερνοεπιθέσεων. Ενημερώσεις: • Ορισμός: Οι ενημερώσεις λογισμικού (συμπεριλαμβανομένων λειτουργικών συστημάτων, προγραμμάτων περιήγησης και εφαρμογών) συχνά περιλαμβάνουν ενημερώσεις κώδικα ασφαλείας που διορθώνουν ευπάθειες και ενισχύουν την άμυνα έναντι απειλών που ανακαλύφθηκαν πρόσφατα. • Σπουδαιότητα: Η τακτική ενημέρωση του λογισμικού διασφαλίζει ότι οι γνωστές αδυναμίες ασφαλείας

Co-funded by the European Union

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

	αντιμετωπίζονται άμεσα, μειώνοντας τον κίνδυνο εκμετάλλευσης από εγκληματίες του κυβερνοχώρου.
Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΕΛΛΑΔΑΣ	1. Σημασία ισχυρών κωδικών πρόσβασης και ελέγχου ταυτότητας δύο παραγόντων Στην Ελλάδα, όπως και σε πολλές χώρες, η χρήση ισχυρών κωδικών πρόσβασης και ελέγχου ταυτότητας δύο παραγόντων (2FA) τονίζεται από τράπεζες και ειδικούς στον τομέα της κυβερνοασφάλειας. Οι ελληνικές τράπεζες συχνά συνιστούν στους πελάτες να δημιουργούν κωδικούς πρόσβασης που περιλαμβάνουν συνδυασμό γραμμάτων (κεφαλαίων και πεζών), αριθμών και ειδικών χαρακτήρων. Ενθαρρύνουν επίσης τη χρήση του 2FA, όπου είναι διαθέσιμο, για να προσθέσετε ένα επιπλέον επίπεδο ασφάλειας πέρα από έναν απλό κωδικό πρόσβασης. Αυτό είναι ιδιαίτερα σημαντικό στην Ελλάδα λόγω της αυξανόμενης υιοθέτησης ψηφιακών τραπεζικών υπηρεσιών, η οποία απαιτεί ισχυρά μέτρα ασφαλείας για την προστασία από απειλές στον κυβερνοχώρο. 2. Αναγνώριση προσπαθειών ηλεκτρονικού ψαρέματος (phishing) και άλλων κοινών απατών Συνιστάται στους Έλληνες να επαγρυπνούν για τις απόπειρες ηλεκτρονικού ψαρέματος, οι οποίες είναι διαδεδομένες σε διάφορες διαδικτυακές πλατφόρμες, συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου, των μέσων κοινωνικής δικτύωσης και των εφαρμογών ανταλλαγής μηνυμάτων. Οι συνήθεις απάτες στην Ελλάδα μπορεί να περιλαμβάνουν δόλια μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα που προσποιούνται ότι προέρχονται από τράπεζες ή κυβερνητικές υπηρεσίες, ζητώντας προσωπικά στοιχεία ή προτρέποντας τους χρήστες να κάνουν κλικ σε κακόβουλους συνδέσμους. Οι εκπαιδευτικές εκστρατείες από τράπεζες και κυβερνητικές υπηρεσίες τονίζουν τη σημασία της επαλήθευσης της αυθεντικότητας των επικοινωνιών πριν από την απάντηση ή την παροχή οποιωνδήποτε προσωπικών πληροφοριών. 3. Προστασία προσωπικών πληροφοριών στο διαδίκτυο Η προστασία των προσωπικών δεδομένων αποτελεί σημαντικό μέλημα στην Ελλάδα, ιδίως με την εφαρμογή του GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων) σε ολόκληρη την ΕΕ. Οι Έλληνες καταναλωτές ενθαρρύνονται να είναι προσεκτικοί σχετικά με την κοινή χρήση προσωπικών

Co-funded by the European Union

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

	στοιχείων στο διαδίκτυο, διασφαλίζοντας ότι οι ιστότοποι είναι ασφαλείς (πρωτόκολλο HTTPS) πριν από την εισαγωγή ευαίσθητων πληροφοριών. Οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα στην Ελλάδα έχουν επίσης εφαρμόσει αυστηρά μέτρα προστασίας δεδομένων για να συμμορφωθούν με τις απαιτήσεις του GDPR, διασφαλίζοντας ότι τα δεδομένα των πελατών αντιμετωπίζονται με ασφάλεια και διαφάνεια. 4. Κατανόηση του ρόλου του λογισμικού ασφαλείας και των ενημερώσεων Στην Ελλάδα, όπως και αλλού, τονίζεται ο ρόλος του λογισμικού ασφαλείας (όπως τα προγράμματα προστασίας από ιούς και τα τείχη προστασίας) για την προστασία από κακόβουλο λογισμικό και άλλες απειλές στον κυβερνοχώρο. Συνιστάται στους Έλληνες καταναλωτές να εγκαθιστούν αξιόπιστο λογισμικό ασφαλείας στις συσκευές τους και να το ενημερώνουν τακτικά. Οι ενημερώσεις σε λειτουργικά συστήματα, προγράμματα περιήγησης και εφαρμογές συχνά περιλαμβάνουν ενημερώσεις κώδικα ασφαλείας που συμβάλλουν στον μετριασμό των τρωτών σημείων και στην ενίσχυση της συνολικής ασφάλειας στον κυβερνοχώρο. 5. Κανονιστικό Πλαίσιο και Συμμόρφωση Τα ελληνικά χρηματοπιστωτικά ιδρύματα λειτουργούν εντός του κανονιστικού πλαισίου της Τράπεζας της Ελλάδος και της Ευρωπαϊκής Κεντρικής Τράπεζας (ΕΚΤ), το οποίο καθορίζει κατευθυντήριες γραμμές για την κυβερνοασφάλεια και την προστασία δεδομένων στις τραπεζικές εργασίες. Η συμμόρφωση με αυτούς τους κανονισμούς διασφαλίζει ότι οι ελληνικές τράπεζες τηρούν υψηλά πρότυπα ασφάλειας και ιδιωτικότητας όταν προσφέρουν ψηφιακές τραπεζικές υπηρεσίες. Οι καταναλωτές ενθαρρύνονται να εξοικειωθούν με τα δικαιώματά τους βάσει αυτών των κανονισμών και να αναφέρουν αμέσως τυχόν ύποπτες δραστηριότητες στην τράπεζά τους ή στις αρμόδιες αρχές.
ΠΑΡΑΔΕΊΓΜΑ	**Αναγνώριση απόπειρας ηλεκτρονικού ψαρέματος (phishing)** Πλαίσιο: Λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου στα εισερχόμενά σας που φαίνεται να προέρχεται από την τράπεζά σας, ζητώντας σας να δώσετε τον κωδικό πρόσβασής

Co-funded by the European Union

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

	σας για να "επαληθεύσετε τον λογαριασμό σας για λόγους ασφαλείας". Το μήνυμα ηλεκτρονικού ταχυδρομείου ισχυρίζεται ότι η μη συμμόρφωση μπορεί να οδηγήσει σε προσωρινή αναστολή του λογαριασμού σας. Βήματα για να αναγνωρίσετε και να απαντήσετε: 1. **Εξετάστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα:** ○ Πλαίσιο: Το μήνυμα ηλεκτρονικού ταχυδρομείου ισχυρίζεται ότι προέρχεται από την τράπεζά σας (π.χ. "YourBankName@gmail.com"). ○ Ανάλυση: Οι νόμιμες τράπεζες χρησιμοποιούν συνήθως τα επίσημα ονόματα τομέα τους για επικοινωνία (π.χ. "@yourbankname.com"). Ένα Gmail ή άλλος γενικός τομέας μπορεί να είναι μια κόκκινη σημαία. 2. **Ελέγξτε για γενικούς χαιρετισμούς και επείγοντα περιστατικά:** ○ Πλαίσιο: Το μήνυμα ηλεκτρονικού ταχυδρομείου ξεκινά με έναν γενικό χαιρετισμό όπως "Αγαπητέ πελάτη" και δίνει έμφαση στον επείγοντα χαρακτήρα. ○ Ανάλυση: Οι νόμιμες επικοινωνίες συχνά χρησιμοποιούν το όνομά σας και διατηρούν επαγγελματικό τόνο. Ο επείγων χαρακτήρας και οι απειλές συνεπειών για μη συμμόρφωση είναι κοινές τακτικές που χρησιμοποιούνται από τους phishers για να σπεύσουν τα θύματα να παράσχουν ευαίσθητες πληροφορίες. 3. **Αναζητήστε ορθογραφικά και γραμματικά λάθη:** ○ Πλαίσιο: Το μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει πολλά ορθογραφικά λάθη και άβολη γραμματική. ○ Ανάλυση: Οι νόμιμες επικοινωνίες από τις τράπεζες είναι συνήθως καλογραμμένες και επαγγελματικές. Τα γραμματικά και ορθογραφικά λάθη είναι ενδείξεις απόπειρας ηλεκτρονικού ψαρέματος (phishing). 4. **Τοποθετήστε το δείκτη του ποντικιού πάνω από συνδέσμους χωρίς να κάνετε κλικ:** ○ Πλαίσιο: Το μήνυμα ηλεκτρονικού ταχυδρομείου περιλαμβάνει έναν σύνδεσμο που υποτίθεται ότι σας κατευθύνει σε έναν ιστότοπο για να εισαγάγετε τον κωδικό πρόσβασής σας. ○ Ανάλυση: Τοποθετήστε το δείκτη του ποντικιού πάνω από τον σύνδεσμο (χωρίς κλικ). Εάν η

Co-funded by the European Union

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

	διεύθυνση URL που εμφανίζεται δεν αντιστοιχεί στον επίσημο ιστότοπο της τράπεζάς σας ή ανακατευθύνει σε ύποπτο τομέα, πιθανότατα πρόκειται για σύνδεσμο ηλεκτρονικού ψαρέματος (phishing). 5. **Επικοινωνήστε απευθείας με την τράπεζά σας:** ○ Πλαίσιο: Υποψιάζεστε ότι το μήνυμα ηλεκτρονικού ταχυδρομείου είναι μια προσπάθεια ηλεκτρονικού ψαρέματος αφού λάβετε υπόψη τα παραπάνω σημεία. ○ Ανάλυση: Αντί να απαντήσετε απευθείας στο email, χρησιμοποιήστε έναν αριθμό επικοινωνίας ή μια επίσημη διεύθυνση URL ιστότοπου που έχετε ήδη για να επικοινωνήσετε με την εξυπηρέτηση πελατών της τράπεζάς σας. Αναφέρετε το ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου και επαληθεύστε αν απαιτείται κάποια ενέργεια στον λογαριασμό σας. 6. **Αναφέρετε την απόπειρα ηλεκτρονικού ψαρέματος:** ○ Ευρύτερο πλαίσιο: Επιβεβαιώνετε με την τράπεζά σας ότι το μήνυμα ηλεκτρονικού ταχυδρομείου ήταν πράγματι απόπειρα ηλεκτρονικού ψαρέματος (phishing). ○ Ανάλυση: Αναφέρετε το μήνυμα ηλεκτρονικού ταχυδρομείου στην επίσημη διεύθυνση ηλεκτρονικού ταχυδρομείου αναφοράς ηλεκτρονικού ψαρέματος της τράπεζάς σας ή επικοινωνήστε με την εξυπηρέτηση πελατών. Αυτό τους βοηθά να αναλάβουν δράση για την προστασία άλλων πελατών από παρόμοιες απάτες.
ΠΡΑΚΤΙΚΗ ΑΣΚΗΣΗ	**Κουίζ: Αναγνώριση προσπαθειών ηλεκτρονικού ψαρέματος** 1. **Ποιο από τα παρακάτω είναι ένα κοινό σημάδι ενός ηλεκτρονικού "ψαρέματος";** Α) Προσωποποιημένος χαιρετισμός με το όνομά σας Β) Επείγουσα γλώσσα που απειλεί με αναστολή λογαριασμού Γ) Επαγγελματική μορφή email από τον επίσημο τομέα της τράπεζας Δ) Σαφείς οδηγίες σχετικά με τον τρόπο διασφάλισης του λογαριασμού σας

Co-funded by the European Union

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

	2. **Τι πρέπει να κάνετε εάν λάβετε ένα email που ζητά τον κωδικό πρόσβασής σας για την επαλήθευση του λογαριασμού σας;** Α) Απαντήστε με τον κωδικό πρόσβασής σας για να επιβεβαιώσετε την ταυτότητά σας Β) Κάντε κλικ στον σύνδεσμο που παρέχεται στο email και εισαγάγετε τον κωδικό πρόσβασής σας Γ) Αγνοήστε το email και διαγράψτε το αμέσως Δ) Καλέστε την τράπεζά σας χρησιμοποιώντας έναν αξιόπιστο αριθμό τηλεφώνου και επαληθεύστε το αίτημα 3. **Γιατί είναι σημαντικό να ελέγχετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα σε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου;** Α) Για να επαληθεύσετε εάν το μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει γραμματικά λάθη Β) Για να διασφαλιστεί ότι το μήνυμα ηλεκτρονικού ταχυδρομείου δεν έχει επισημανθεί ως ανεπιθύμητο Γ) Για να επιβεβαιώσετε εάν το μήνυμα ηλεκτρονικού ταχυδρομείου προέρχεται από νόμιμη πηγή Δ) Για να αναφέρετε το μήνυμα ηλεκτρονικού ταχυδρομείου στον πάροχο ηλεκτρονικού ταχυδρομείου σας 4. **Τι πρέπει να κάνετε εάν υποψιάζεστε ότι ένα μήνυμα ηλεκτρονικού ταχυδρομείου είναι απόπειρα ηλεκτρονικού ψαρέματος;** Α) Προωθήστε το email σε όλες τις επαφές σας για να τις προειδοποιήσετε Β) Κάντε κλικ σε οποιονδήποτε σύνδεσμο στο email για να επαληθεύσετε τη γνησιότητά του Γ) Καλέστε απευθείας την τράπεζα ή το χρηματοπιστωτικό σας ίδρυμα για να επαληθεύσετε το αίτημα Δ) Απαντήστε στο email με τα προσωπικά σας στοιχεία για επαλήθευση 5. **Ποιο από τα παρακάτω αποτελεί κόκκινη σημαία για ένα μήνυμα ηλεκτρονικού "ψαρέματος";** Α) Η διεύθυνση ηλεκτρονικού ταχυδρομείου αντιστοιχεί στον επίσημο τομέα της τράπεζάς σας Β) Το email περιέχει γραμματικά και ορθογραφικά λάθη

Co-funded by the European Union

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

	Γ) Το μήνυμα ηλεκτρονικού ταχυδρομείου παρέχει σαφείς οδηγίες σχετικά με τον τρόπο προστασίας του λογαριασμού σας Δ) Το email περιλαμβάνει σύνδεσμο προς την επίσημη ιστοσελίδα της τράπεζας για περισσότερες πληροφορίες **Απαντήσεις:** 1. Β) Επείγουσα γλώσσα που απειλεί με αναστολή λογαριασμού 2. Δ) Καλέστε την τράπεζά σας χρησιμοποιώντας έναν αξιόπιστο αριθμό τηλεφώνου και επαληθεύστε το αίτημα 3. Γ) Για να επιβεβαιώσετε εάν το μήνυμα ηλεκτρονικού ταχυδρομείου προέρχεται από νόμιμη πηγή 4. Γ) Καλέστε απευθείας την τράπεζα ή το χρηματοπιστωτικό σας ίδρυμα για να επαληθεύσετε το αίτημα 5. *Β) Το email περιέχει γραμματικά και ορθογραφικά λάθη*
ΘΕΜΑΤΑ ΠΡΟΣ ΣΥΖΉΤΗΣΗ	**Ερώτηση προβληματισμού 1** Θα πρέπει οι τράπεζες να είναι αποκλειστικά υπεύθυνες για την αποζημίωση των θυμάτων ηλεκτρονικής απάτης ή θα πρέπει οι πελάτες να φέρουν κάποια ευθύνη για τη διασφάλιση της δικής τους ασφάλειας στο διαδίκτυο; **Ερώτηση προβληματισμού 2** Πώς μπορούν τα άτομα να εξισορροπήσουν την ευκολία των ψηφιακών συστημάτων πληρωμών με την ανάγκη για ισχυρά μέτρα ασφαλείας;
ΣΧΌΛΙΑ	

Co-funded by the European Union

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