Stadt Senioren Rat Heidenheim e.V.

Heidenheim an der Brenz

Internet- und PC-Unterstützung für die Generation 50plus

HERZLICH WILLKOMMEN ZUM VORTRAG AM 03.06.2024

FREIER EINTRITT

Eine Spendenbox ist aufgestellt.

Aufgrund der aktuellen Situation mit derzeit vermehrt vielen Betrugsfällen und Schockanrufen wird Sie Kriminalhaupt-kommissar Christian Quattrone Polizeipräsidium Ulm, Referat Prävention informieren, wie Sie sich davor schützen und verhalten können.

Die Teilnehmer erhalten kostenlose Broschüren

Bei kostenlosen Vorträgen (freier Eintritt) werden keine persönlichen Daten erfasst und es wird kein Dossier des Vortrags versendet.

BETRUGS MASCHEN

INFORMATIONSVERANSTALTUNG

Wann:	Montag, 03.06.2024, 10.00 Uhr
Wo:	Heidenheim, Rathaus (Emil-Ortlieb-Saal)
Referenten:	Kriminalhauptkommissar Christian Quattrone, Polizeipräsidium Ulm, Referat Prävention

Zusatzthema:
Tipps zum Einbruchschutz

In Kooperation mit
POLIZEI BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM ULM

www.stsr-heidenheim.de

Stadt Senioren Rat Heidenheim e.V.

Der Stadtseniorenrat fördert und organisiert mit dem Projekt „Internet- und PC-Unterstützung für die Generation 50plus“ Vorträge und individuelle persönliche Hilfestellung
- auch für Einsteiger:innen -
zu allen Themen rund um die digitale Welt zu Computer, Tablets und Smartphones für Betriebssysteme Windows, Android und Apple-Geräten.

Ein Team der ehrenamtlichen Internetlotsen steht Ihnen immer montags von 10-12 Uhr (außer in den Ferien und an Vortrags-Terminen) mit neutraler Beratung und Unterstützung zur Seite, bei offenen Treffpunkten in Räumen des Bürgerhauses Heidenheim im 1.Stock, Raum 102 + 103

www.stsr-heidenheim.de

Stadt Senioren Rat Heidenheim e.V.

Die ehrenamtlichen Internetlotsen vom Stadtseniorenrat helfen Ihnen, Ihre Daten vom PC auf externe Laufwerke wie Festplatten oder Sticks zu übertragen und somit zu sichern.

Auch Ihre Fotos / Bilder / Videos und Dokumente von Ihrem Smartphone, sollten Sie auf externe Laufwerke überspielen und sichern.

Kommen Sie zu den Sprechstunden ins Bürgerhaus und bringen Sie Ihre Geräte mit allen dazugehörigen Kabeln mit, damit wir Ihnen beim Sichern Ihrer Daten helfen können.

Informationen, Termine, kostenlose Downloads und Tipps finden Sie auf unserer Homepage unter www.stsr-heidenheim.de

Auf den nachfolgenden Seiten haben wir für Sie diverse Tipps zum heutigen Thema zusammengestellt, die Sie auf unserer Homepage kostenfrei herunterladen können auf der Seite DOWNLOADS.

Tipps von der Verbraucherzentrale zu Schockanrufen

Die *Verbraucherzentrale* Bremen hat einige gute Verhaltenstipps zum Umgang mit KI-generierten Sprachnachrichten von Angehörigen zusammengestellt:

- **Versuchen Sie unbedingt, ruhig zu bleiben, auch wenn dies in der Stresssituation nicht einfach ist**
- **Treffen Sie auf keinen Fall überstürzte Entscheidungen, nur weil Sie am Telefon unter Druck gesetzt werden**
- **Beenden Sie das Gespräch und rufen den vermeintlichen Anrufer zurück, um sich zu versichern, ob tatsächlich eine Notlage besteht**
- **Stellen Sie im Gespräch Fragen nach bestimmten Orten oder Gegebenheiten, die nur die betroffene Person kennt oder auch „dumme“ Fragen, die nichts mit dem bisherigen Gespräch zu tun haben**
- **Geben Sie in Telefonaten keine persönlichen Informationen und Details preis**
- **Notieren Sie sich Datum und Uhrzeit des Anrufs, die Umstände und falls vorhanden die angezeigte Rufnummer und erstatten Sie Strafanzeige bei der Polizei, damit eine strafrechtliche Verfolgung möglich ist**

Stadt Senioren Rat Heidenheim e.V.

Ein wichtiger Tipp:

Vereinbaren Sie unbedingt ein Codewort innerhalb Ihrer Familie, dass sie im Bedarfsfall abfragen können. Ein Codewort bzw. Safeword innerhalb der Familie dient als effektiver Schutzmechanismus, um Betrugsversuche schnell zu identifizieren und abzuwehren.

Betrüger entwickeln ständig neue Methoden, um ihre Opfer zu täuschen. Deshalb ist es wichtiger denn je, wachsam zu sein und den Kriminellen den Wind aus den Segeln zu nehmen – beispielsweise mit einem Codewort bzw. Safeword.

Raffinierte Betrugsmethoden:
Von Kautionsforderungen bis zu KI-gestützten Anrufen
Die Täter schrecken vor nichts zurück. Sie täuschen vor, dass Angehörige in schwere Unfälle verwickelt sind, für die hohe Kautionssummen verlangt werden, oder dass es sich um medizinische Notfälle handelt, für die ebenfalls hohe Summen bezahlt werden müssen.

Auch die Betrugsmasche „Hallo Mama/Papa“ über **WhatsApp** kursiert schon länger. Sie fordert immer wieder Opfer, die nur ihren vermeintlichen Kindern und Enkeln helfen wollen.

Quelle: https://www.mimikama.org/codewort-safeword-familie/

Warum ein Familien-Safeword oder Codewort so wichtig ist
Um solchen Betrügereien einen Schritt voraus zu sein, ist es sinnvoll, innerhalb der Familie und im Freundeskreis ein Codewort / Safeword zu verwenden. Dieses Codewort dient als unverwechselbares Signal und kann helfen, echte von gefälschten Anfragen zu unterscheiden. So schützen Sie sich und Ihre Angehörigen auf einfache, aber wirkungsvolle Weise vor finanziellen und emotionalen Schäden.

Auswahl und Einrichtung eines wirksamen Safewords
Die Wahl eines geeigneten Codeworts ist entscheidend. Es sollte einzigartig und nicht leicht zu erraten sein, aber einfach genug, um es sich zu merken. Nach der Wahl ist es wichtig, dass alle Familienmitglieder und engen Freunde das Wort kennen und wissen, wann und wie es zu verwenden ist.

Gebrauch des Codeworts in kritischen Situationen
Das Safeword kann in vielen Situationen eingesetzt werden: wenn ein Kind von einer fremden Person abgeholt wird, bei ungewöhnlichen Hilfegesuchen oder zur Überprüfung der Echtheit von E-Mails und Telefonanrufen. Es bietet eine schnelle und zuverlässige Methode, um die Authentizität einer Anfrage zu überprüfen.

Quelle: https://www.mimikama.org/codewort-safeword-familie/

Vertraulichkeit wahren und bei Bedarf anpassen

Es ist wichtig, dass das Codewort innerhalb des vertrauten Kreises bleibt. Wenn es öffentlich bekannt wird, verliert es seine Wirksamkeit und kann sogar ausgenutzt werden. Bei Verdacht auf Kompromittierung oder Verlust der Wirksamkeit sollte das Safeword geändert werden.

Fazit: Ein einfacher Schritt für mehr Sicherheit

Die Einführung eines Familien-Safewords ist ein kleiner, aber entscheidender Schritt für Ihre Sicherheit in einer zunehmend digitalisierten Welt. Es bietet nicht nur Schutz vor Betrügern, sondern stärkt auch das Bewusstsein und die Zusammenarbeit innerhalb der Familie.

Quelle: **https://www.mimikama.org/codewort-safeword-familie/**

Am 6. Februar 2024 war Safer Internet Day - Tag des sichereren Internets, ein Aktionstag für mehr Online-Sicherheit.

Weltverbrauchertag 2024
Quelle: https://www.t-online.de/digital/sicherheit/id_100303360/weltverbrauchertag-das-sind-die-groessten-fallen-im-internet.html

Das sind die größten Fallen im Internet – und so können Sie sich schützen.

Die Bedrohung im Cyberraum ist "so hoch wie nie zuvor", heißt es im Lagebericht der IT-Sicherheit 2023 vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Neue Technologien wie Künstliche Intelligenz (KI) bieten jede Menge Chancen, bergen aber auch Gefahren.

Existenzielle Bedrohung für Unternehmen
Gerade für Unternehmen seien die Folgen eines Cyberangriffs oft fatal, so der Experte weiter. "Wenn eine Firma Wochen braucht, um ihre Datensätze nach einem Hack wiederherzustellen, dann ist sie in der Regel pleite. Das heißt: Hier müssen Unternehmen rechtzeitig vorsorgen."

Doch auch für Privatnutzer kann ein falscher Klick schwerwiegend sein. Plötzlich sind sämtliche Daten wie Dokumente, Fotos und Videos weg oder Betrüger missbrauchen Kreditkartendaten. Hier die größten Fallen, die im Internet lauern:

Phishing-Betrug: Phishing-Attacken zielen darauf ab, persönliche Informationen wie Benutzernamen, Passwörter und Kreditkartennummern zu stehlen. Betrüger geben sich oft als vertrauenswürdiges Unternehmen aus und senden gefälschte E-Mails oder erstellen gefälschte Websites, um Nutzer zur Preisgabe sensibler Daten zu verleiten.

Hier ein paar Tipps, woran Sie die Mails erkennen.

Malware und Viren: Das Herunterladen von Dateien aus unsicheren Quellen kann dazu führen, dass schädliche Software (Malware) auf Ihren Computer gelangt. Diese Programme können sensible Daten stehlen, das System beschädigen oder für andere bösartige Aktivitäten genutzt werden.

Identitätsdiebstahl: Kriminelle versuchen, Ihre persönlichen Informationen zu stehlen, um in Ihrem Namen Transaktionen durchzuführen oder Verbrechen zu begehen. Dies kann durch Phishing, Hacking oder den Diebstahl von physischen Geräten erfolgen.

Fake Shops: Betrüger erstellen gefälschte Onlineshops, um Verbraucher dazu zu verleiten, Produkte zu kaufen, die nie geliefert werden.

Hier bekommen Sie Tipps, woran Sie solche Fake Shops erkennen.

Buy Now, Pay Later: Diese vermeintlichen Angebote sollen es Käufern ermöglichen, ihre Einkäufe später zu bezahlen. Allerdings steckt hinter dieser Masche oft ein kostenpflichtiger Kreditvertrag von Drittanbietern. Bei mehreren kleinen Krediten können Verbraucher schnell den Überblick verlieren und aufgrund der hohen Zinsen überschulden.

Soziale Netzwerkfallen: Cyberkriminelle nutzen soziale Netzwerke, um persönliche Informationen zu sammeln und Phishing-Angriffe durchzuführen. Wenn Nutzer zum Beispiel die Namen ihrer Kinder oder Haustiere öffentlich machen, können Angreifer daraus mögliche Passwörter generieren.

Ransomware: Ransomware ist eine Form von Malware, die die Daten auf einem Computer verschlüsselt und dann Lösegeld für die Entschlüsselung verlangt.

Öffentliches WLAN: Die Nutzung öffentlicher WLAN-Netzwerke kann riskant sein, da sie oft ungesichert sind. Kriminelle könnten den Datenverkehr über diese Netzwerke überwachen und persönliche Informationen abfangen.

Gefälschte Bilder und Videos: Betrüger verbreiten mithilfe von KI erstellte Bilder, Audio- und Videodateien im Internet und den sozialen Medien, um Verwirrung zu stiften, Falschaussagen zu streuen und Meinungen zu beeinflussen.
Um sich vor diesen Gefahren zu schützen, ist es wichtig, aufmerksam zu sein, sicherheitsbewusst zu handeln und regelmäßige Updates durchzuführen. Auch eine gute Antivirensoftware und eine sichere Internetverbindung tragen dazu bei, das Risiko zu minimieren.

Hier sind weitere Tipps, um sich vor den Gefahren im Internet zu schützen:
Starke und individuelle Passwörter verwenden: Verwenden Sie für jeden Onlinedienst ein einzigartiges und starkes Passwort. Ein starkes Passwort sollte mindestens acht Zeichen lang sein sowie Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.

Zwei-Faktor-Authentifizierung (2FA) aktivieren: Aktivieren Sie die Zwei-Faktor-Authentifizierung, wo immer es möglich ist. Dies bietet eine zusätzliche Sicherheitsebene, indem ein zweiter Verifizierungsschritt erforderlich ist.

Software regelmäßig aktualisieren: Halten Sie Ihr Betriebssystem, Ihren Browser, Ihre Antivirensoftware und alle anderen Programme auf Ihrem Computer oder Mobilgerät auf dem neuesten Stand. Aktualisierte Software schließt oft Sicherheitslücken.

Vorsicht bei E-Mails: Seien Sie skeptisch gegenüber unerwarteten E-Mails, insbesondere solchen, die Links oder Anhänge enthalten. Überprüfen Sie sorgfältig die E-Mail-Adresse des Absenders und vermeiden Sie das Klicken auf verdächtige Links.

Sichere Verbindungen nutzen: Vermeiden Sie die Nutzung unsicherer WLAN-Netzwerke. Wenn Sie öffentliche WLAN-Netzwerke verwenden müssen, nutzen Sie eine VPN-Verbindung (Virtual Private Network), um Ihre Daten zu schützen.

Sicherheitseinstellungen in sozialen Netzwerken überprüfen: Überprüfen Sie regelmäßig die Datenschutzeinstellungen Ihrer Konten in sozialen Netzwerken und begrenzen Sie den Zugriff auf persönliche Informationen.

Informationen kritisch prüfen: Seien Sie vorsichtig beim Teilen persönlicher Informationen im Netz. Überlegen Sie, ob die angeforderten Daten wirklich notwendig sind, und teilen Sie sie nur mit vertrauenswürdigen Quellen.

Aufmerksamkeit bei Onlinekäufen: Achten Sie bei Online-Transaktionen auf sichere Webseiten, die mit "https://" beginnen. Vermeiden Sie außerdem den Zugriff auf sensible Informationen über öffentliche Computer.

Konto im Blick halten: Überprüfen Sie regelmäßig Ihre Bank- und Kreditkarten-abrechnungen, um ungewöhnliche Aktivitäten schnell zu erkennen. Melden Sie verdächtige Aktivitäten sofort.

Bildung und Aufklärung: Halten Sie sich über die neuesten Online-Bedrohungen auf dem Laufenden und bilden Sie sich fort. Aufklärung ist ein wichtiger Schutz vor Betrügereien.
Doch selbst bei aller Vorsicht bleibt es manchmal nicht aus, dass persönliche Daten geklaut werden. So werden mitunter auch die Unternehmen gehackt, bei denen unsere Informationen gespeichert werden. In jedem Fall ist es dann wichtig, den Angriff zu melden und so schnell wie möglich das eigene Passwort zu ändern.

Back-ups: Erstellen Sie regelmäßig Back-ups Ihrer wichtigsten Daten auf externen Laufwerken oder in der Cloud. Dies kann Ihnen helfen, die Daten im Falle von Ransomware-Angriffen wiederherzustellen. Oder wenn die Festplatte kaputtgeht, der Laptop verloren oder geklaut wird.

Quelle: https://www.t-online.de/digital/sicherheit/id_100303360/weltverbrauchertag-das-sind-die-groessten-fallen-im-internet.html