Infoblatt zu „zusammen digital"

Digitales Bürgerkonto (z. B. BayernID, BundID)

Was ist das digitale Bürgerkonto?

- Einheitlicher Zugang zu allen Online-Verfahren der öffentlichen Verwlatung
- Ein Postfach, in das man Nachrichten von Behörden erhalten kann, sowie auch digitale Bescheide
- Einmal hinterlegte Daten müssen nicht erneut angegeben werden (z. B. Name, Adresse, Geburtsdatum)

Für was wird dieses benötigt?

- Verwaltungsleistungen können online beantragt werden
- Nachrichten können von Behörden erhalten werden
- Einfache, sichere Identifizierung in Online-Verfahren

Kempten.de/digital

Wie kann ich mich für ein digitales Bürgerkonto registrieren?

- Online-Ausweisfunktion des Personalausweises
- ELSTER-Zertifikat
- Europäische eID
- Benutzername/ Passwort (ist geringstes Authentifzierungsmittel, daher kein Ausweisersatz)

Was ist die Online-Ausweisfunktion?

- Mit der Online-Ausweisfunktion kann man sich sicher ausweisen bei der Beantragung von digitalen Verwaltungsleistungen
- Ersetzt die Unterschrift auf dem Papierantrag

Online-Bezahlmöglichkeiten bei der Stadt Kempten (Allgäu):

Kreditkarte, GiroPay, SEPA-Lastschrift, PayPal

- Ablauf bei der **Kreditkarte**: Eingabe der Kreditkartennummer (16-stellige Kreditkartennummer, Gültigkeitsdatum, Name, 3-stellige VPN (Sicherheitsnummer), Betrag wird nicht sofort vom Konto abgebucht, sondern hat einen monatlichen Kreditrahmen (=Betrag wird nicht sofort vom Konto abgezogen), es gibt verschiedene Anbieter bei der Stadt Kempten werden VISA und MasterCard akzeptiert

- Bezahlvorgang bei **SEPA-Lastschrift**: Eingabe der Kontodaten, anschließend wird durch ein SEPA-Lastschriftmandat die Abbuchung des Rechnungsbetrags vom Konto abgebucht. , Lastschriften können ohne Angaben von Gründen 8 Wochen zurückgegeben werden.

- **GiroPay**= Online-Bezahlfunktion, als sicheres Gegenstück zu dritten Zahlungsanbietern Registrierung erfolgt im Online-Banking, hierbei wird Anmeldename und Passwort vergeben, Bezahlvorgang erfolgt somit über Online-Banking.
- **PayPal**: kostenlose Registrierung bei PayPal für ein „digitales Konto" mit Hinterlegung der Bankdaten oder Kreditkartendaten, keine Übertragung persönlicher Daten an den „Händler", Eingabe der E-Mail-Adresse beim Bezahlvorgang

Gefahren im Internet:

Was gibt es für Gefahren?

- Online-Betrug (Phishing, Identitätsdiebstahl, Social Engineering)
- Angriffe (Malware-Infektionen, Ransomware Angriffe)

Phishing:

- Bekannteste Methode: Phishing-Mails
- Vorgehen: Angreifer geben sich als vertrauenswürdige Unternehmen aus und versuchen, Benutzer zur Preisgabe sensibler Informationen wie Passwörter, Kreditkartendaten oder persönliche Daten zu verleiten. Dies geschieht häufig durch gefälschte E-Mails, Websites oder Social Media Nachrichten
- Ziel: Finanzinformationen, Zugangsdaten oder andere sensible Daten herauszufinden, um Identitätsdiebstahl oder Betrug zu begehen.
- Gegenmaßnahmen: E-Mails genau durchlesen, und auf den Absender achten, meist keine direkten Ansprache wie beispeilsweise Sehr geehrter Herr xy, sondern Hallo.., bei unbekannten Absendern auf keine Links klicken oder Anhänge öffnen, Antivirus-Software installieren, regelmäßig System-Updates installieren, um auf dem neuesten Stand zu sein.

Identitätsdiebstahl:

- Vorgehen: Angreifer versucht persönliche Informationen wie Name, Adresse, Sozialversicherungsnummer oder Kreditkartendaten zu stehlen und sich anschließend mit diesen Daten als jemand anderes auszugeben.
- Ziel: im Namen des Opfers Waren und Dienstleistungen kaufen, Kredite aufnehmen, Schädigung des Rufs, Identität einer anderen Person für illegale Zwecke nutzen
- Gegenmaßnamen: Kontoausgänge regelmäßig kontrollieren, keine persönlichen Daten weitergeben, sichere Passwörter verwenden, 2-Faktor-Authentifizierung verwenden (Passwort und Personalausweis), keine Daten auf unseriösen Websites angeben

Social Engineering:

- Vorgehen: Angreifer versucht persönliche Informationen wie Name, Adresse, Sozialversicherungsnummer oder Kreditkartendaten zu stehlen und sich anschließend mit diesen Daten als jemand anderes auszugeben

- Ziel: Im Namen des Opfers Waren und Dienstleistungen kaufen, Kredite aufnehmen, Schädigung des Rufs, Identität einer anderen Person für illegale Zwecke zu verwenden
- Gegenmaßnahmen: Kontoausgänge regelmäßig kontrollieren, keine persönlichen Daten weitergeben, sichere Passwörter verwenden, 2-Faktor-Authentifizierung aktivieren, keine Daten auf unsicheren Websites angeben

Malware-Infektionen:

Umfasst Viren, Trojaner, Würmer und andere bösartige Programme. Sie werden oft unbemerkt auf einem System installiert und können Schaden anrichten, wie Datenverlust, Systemabstürze oder den Fernzugriff auf das Gerät ermöglichen.

- Vorgehen: Die Malware wird über unsichere Downloads, infizierte E-Mail-Anhänge, Drive-by-Downloads auf bösartige Websites oder über infizierte externe Geräte verbreitet
- Ziel: Diebstahl persönlicher Informationen, die Kontrolle über das Gerät des Benutzers oder das Erzielen finanzieller Gewinne durch Lösegeldforderungen
- Gegenmaßnahmen: regelmäßige Updates, Antiviren-Software, regelmäßige Backups wichtiger Daten, Vorsichtig beim Herunterladen von Dateien

Ransomware-Angriffe:

Ransomware ist eine Art Malware, die die Daten eines Benutzers verschlüsselt und Lösegeld fordert, um die Daten wiederherzustellen.

- Vorgehen: Ransomeware kann durch das Öffnen von infizierten E-Mail-Anhängen, das Besuchen infizierter Websites oder das Herunterladen von bösartigen Dateien verbreitet werden
- Ziel: das Ziel von Ransomeware-Angriffen ist es, finanziellen Gewinn zu erzielen, indem das Opfer zur Zahlung eines Lösegeldes gezwungen werden
- Gegenmaßnahmen: regelmäßige Updates, Antiviren-Programme, regelmäßige Backups wichtiger Daten, diese offline speichern. Vorsicht beim Öffnen von E-Mail-Anhängen oder Dateien aus unsicheren Quellen

Vielen Dank für Ihr Feedback zur Beratungstheke „zusammen digital"