willkommen

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

1. Digitale Sprechstunde Gemünden

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Gefördert durch:

RheinlandPfalz
MINISTERIUM FÜR ARBEIT, SOZIALES, TRANSFORMATION UND DIGITALISIERUNG

Unterstützt von:

Medienanstalt Rheinland-Pfalz

Agenda

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

1 Sind noch Fragen zur Infoveranstaltung vom 12.10.2024

2 Heutige Themen

3 Ihre Wünsche für die nächste Sprechstunde **???**

Wer die Präsentation(en) per PDF erhalten möchte,
bitte formlose E-Mail an di-bo-westerburg@online.de

Fragen zur Infoveranstaltung

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Anregungen, Kritik
- Was sollten wir ändern, was verbessern?
- Gerne auch per Mail an di-bo-westerburg@online.de

Ihre offenen Themenwünsche

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- ➔ E-Mail (Anhänge, … auf Handy empfangen bzw. senden
- ➔ Cyberangriffe, Hackerangriffe, Gefahren im Internet
- ➔ Drucken mit dem Handy, Handy mit Drucker verbinden
- ➔ ePA für alle – Einführung zum 15.01.2025 AKTUELL
- ➔ Datenschutz, Datensicherheit, Sicherungskopien erzeugen und einlesen
- ➔ Cloudspeicher
- ➔ QR-Code
- ➔ Datenmüll entfernen, Handy „aufräumen“
- ➔ Briefe schreiben – Tipps und Tricks
- ➔ Betrugsmaschen, Fakeshops

Heutige Themen

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Cyberangriffe – Gefahren der Digitalen Welt

Sichere Passworte bilden – die man sich auch merken kann

Cyberangriffe
– es kann jeden treffen!!!

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Bundesamt
für Sicherheit in der
Informationstechnik

Digital Botschafterinnen
& Botschafter
Rheinland-Pfalz

Die Lage der IT-Sicherheit in Deutschland 2024

Datum 12.11.2024

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) jährlich einen umfassenden Überblick über die Bedrohungen im Cyberraum. Im Bericht für das Jahr 2024 kommt die Cybersicherheitsbehörde des Bundes zur Einschätzung: Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend.

Cyberangriffe???

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Als Cyberangriff bezeichnet man den Versuch

- Computer (oder andere Endgeräte) außer Betrieb zu setzen
- Daten zu stehlen
- Angegriffenes Computersystem für weitere Aktionen nutzen

Cyberangriffe???

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

2022 betrug der Gesamtschaden durch Cyberangriffe den Gegenwert von 724 Passagierflugzeugen

309000

Es werden **täglich** etwa 309000 neue Schad-Software-Anwendungen programmiert (teils auch mit KI)
Quelle: BSI 12.11.24

Welche Ziele verfolgen die Angreifer?

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Datendiebstahl
- Datenmissbrauch
- Datenmanipulation
- Kontrolle über Fremdgeräte
- Destabilisierung von Firmen und Organisationen

Welche Intention verfolgt Ihr mit den Angriffen?

… hier wurden 3150 Hacker aus 120 Ländern befragt

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Reiz der Herausforderung 68%
- Finanzielle Anreize 53%
- Neue Techniken erlernen 51%
- Helfen und beschützen 20%

Gegenseitiges Wettrüsten

Warum bin ich interessant für Hacker?

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Im großen Stil werden natürlich Unternehmen angegriffen große Konzerne, aber auch kleine Kreis- und Gemeindeverwaltungen usw.
- Diese gestohlenen Daten oder auch Teilpakete davon werden gegen „Geld“ angeboten und verkauft
- So gelangen dann auch die Daten des „kleinen Mannes“ in den Umlauf der Cyberkriminalität
- So wird die ganze Bandbreite der Kriminellen mit den Daten „versorgt“

➔ wurde z.B. mein Energieversorger gehackt – sind meine Daten auch dabei

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

„Kleinkriminelle“ hacken aber auch

- Foren
- Soziale Netzwerke (Facebook, X usw.)
- Serviceportale

Angriffe durch Nachrichten

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Phishing klassisch über E-Mail Anhänge oder Links
  Versand gefälschter E-Mails, die Menschen dazu verleiten sollen, auf einen Betrug hereinzufallen. Phishing-Mails zielen häufig darauf ab, dass die Nutzer Finanzinformationen, Zugangsdaten oder andere sensible Daten preisgeben.

- Smishing SMS oder andere Textnachrichten Link
  Versand von Textnachrichten SMS, Aufforderung einen manipulierten Link zu öffnen

Computer Emergency
Response Team

https://www.naspa.de/de/home/privatkunden/online-banking/sicherheit-im-internet/s-cert-meldungen.html

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Rechnung fehlgeschlagen - Konto gesperrt

NETFLLIX

Hi [redacted]

Wir haben Probleme mit Ihren aktuellen Rechnungsinformationen. Wir werden es erneut versuchen, aber in der Zwischenzeit möchten Sie möglicherweise Ihre MASTERCARD in Ihren Zahlungsdetails aktualisieren.

JETZT KONTO AKTUALISIEREN

Wir sind hier, um Ihnen zu helfen, wenn Sie es brauchen. Besuche den Hilfezentrum für mehr info oder kontaktiere uns.

Deine Freunde bei Netflix

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Stadtsparkasse München

Sehr geehrter Kunde,

Da gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München durchzuführen.
Der Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeitarbeit,
Administration der Stadtsparkasse München

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Angriffe über das Telefon

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Vishing *(„wisching“)* Telefonanruf Kein technischer Schutz möglich
  „von angeblichen Microsoft-Mitarbeitern“

„Vishing“ ist die Abkürzung für „Voice Phishing“ und bezeichnet Phishing-Anrufe per Telefon. Visher verwenden gefälschte Telefonnummern, stimmverändernde Software, Textnachrichten und Social Engineering, um ihre Opfer dazu zu bringen, vertrauliche Informationen preiszugeben

Social Engineering hier geht es um die zwischenmenschliche Beeinflussung einer Person. Dabei versucht der Hacker das Vertrauen des Opfers zu gewinnen und dadurch an Daten zu gelangen (meistens Konto- oder Kreditkartendaten)

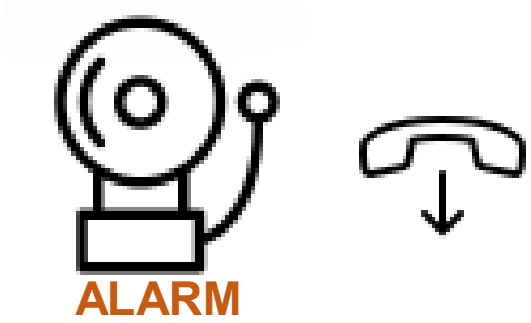
Achtung – da sind Profis am Werk

Psychologische Manipulation

Angriffe über das Telefon

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Das Telefon klingelt, Sie heben ab
- Ein angeblicher Mitarbeiter dieser Firma meldet sich in gebrochenem Deutsch (indisch, englisch usw.)
- „Mir ist aufgefallen“, dass
  - Ihre Lizenz bald abläuft
  - Ihr Computer von einem gefährlichen Virus oder Trojaner befallen wurde
  - Sie sofort ein Sicherheitsupdate des Betriebssystems ausführen müssen
- Dann möchte der angebliche Mitarbeiter per „**Fernwartung**“ auf Ihren Rechner zugreifen
  - um den Rechner zu prüfen
  - das Update auszuführen
  - den Virus/Trojaner zu entfernen



Koppelung mit Schockanruf

Angriffe über Schad-Software

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Viren
- Würmer
- Trojaner
- Spyware (Spione)

Schäden und Beeinträchtigungen der Geräte

➔ Daten werden beschädigt
➔ Daten werden gelöscht
➔ Daten werden infiziert
➔ Infizierte Daten verbreiten sich automatisch
➔ Computer- und Stabilitätsprobleme „Performance“
➔ Öffnet Ihren Computer für Hackerangriffe
➔ Ausspähung von Surfverhalten

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

This **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files…

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in other currency.

Click Next to select the method of payment.

Any attempt to remove or damage this software will lead to immediate destruction of the private key by server.

LÖSEGELDFORDERUNG

Angriffe über Schad-Software

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Seien Sie vorsichtig!!! **GESUNDES MISSTRAUEN!!!**

➔ **Unbekannten E-Mails mit Anhängen**

➔ **Unbekannten E-Mails mit Verlinkungen**

➔ **Austausch von externen/mobilen Datenträgern/Datenquellen**

➔ **Unbekannten Fernwartungs-Zugriffen**

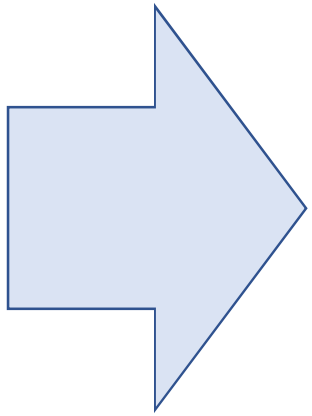
➔ **Unbekannten QR-Codes**

➔ **Rundmails (Einladungen / Gewinncoupons / Gewinnbenachrichtigungen**

Sofortmaßnahmen erforderlich

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Viren
- Würmer
- Trojaner
- Spyware



➔ **Kein** Online Banking mehr über dieses Gerät
➔ Wiederherstellungs-Maßnahmen erforderlich
➔ Schad-Software entfernen, entfernen lassen
➔ Bei Zweifeln, Rechner neu aufbauen
„Platt Machen“ – Neuinstallation – „sicher ist sicher“

Schutzmaßnahmen „ständig“

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Aktuelles, sauberes „Original-Betriebssystem“ betreiben
- Sicherheitsupdates, Patches, regelmäßig für alle Anwendungen ausführen
- Setzen Sie eine Personal-Firewall, besser noch VPN ein
- Installation einer Antiviren-Software, regelmäßig Updates
- Vorsicht mit Anhängen von E-Mails
- **Gesundes Misstrauen und Vorsicht** beim Einsatz von unbekannten CD´s, USB-Sticks, externen Festplatten, Links, QR-Codes und E-Mailanhängen
- Halten Sie sich von „zwielichtigen Websites“ fern
- Installieren Sie nur Originalsoftware von sicherer, bekannter Herkunft

Schutzmaßnahmen „Fortgeschrittene“

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Sicherste Netzwerkumgebung (Router, WLAN-Gastzugang, Nachtabschaltung SSID aus, Passworte ändern usw.)
- Einsatz von Tools gegen Malware, Würmer, Trojaner usw.
- Benutzer anlegen, Rechte und Berechtigungen vergeben und Standard-Passworte und -Berechtigungen löschen, Recht „Jeder“ löschen, nur mit dem angelegten Benutzerrecht arbeiten, Berechtigungen und Freigaben administrieren
- Löschen Sie die Standardrechte und Berechtigungen des Administrators
- Erstellen Sie regelmäßig Datensicherungen auf sichere Datenträger
- Lagern Sie Ihre Daten an einem sicheren Ort (Brand, Wasser, Diebstahl)

Sofortmaßnahmen - Bemerkungen

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Wir können auch mit noch so ausgestalteten Schutzmaßnahmen NIE einen hundertprozentigen Schutz erreichen!!!
- Wir befinden uns immer in einer Welt, wo EIN Internet, für Anwender und Kriminelle, gleichzeitig zur Verfügung gestellt wird
- Wir dürfen aber auch nicht die Gefahren in der digitalen Welt, also überwiegend Internet und beim Online Banking, immer höher gewichten, wie unsere Gefahren in unserer realen Welt.

Heutige Themen

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Cyberangriffe – Gefahren der Digitalen Welt

Sichere Passworte bilden – die man sich auch merken kann

Dieses Thema wurde auf den 12.12.2024 verschoben

Kontaktmöglichkeiten

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

- Michael Roth
  - di-bo-westerburg@online.de
  - **02663-9649942**

- Weitere Kontakte und Informationen gibt es auf der Webseite **https://digital-botschafter.Cyberangriffe/**
  („Veranstaltungen“ – werden alle aktuellen Termine angezeigt)
- Mitteilungen im Wäller Wochenspiegel beachten
- Wir kontaktieren Sie gerne per E-Mail zu Veranstaltungen

Ihre Themenwünsche für **12.12.2024**

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Themenwünsche:

Sichere Passworte bilden – die man sich auch merken kann

Router und Telefon administrieren – Bestimmte Nummern blockieren

Handypass – Polizei Köln NRW

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Zeit für Ihre Fragen

Gute Fahrt – schönen Abend noch!

Digital Botschafterinnen & Botschafter Rheinland-Pfalz

Vielen Dank für Ihren Besuch
Wir freuen uns auf den **12.12.2024**