Cyber Report April 2020

cysmo powered by ppi

Achtung, es wurden Leaks gefunden!

max@mustermann.de
ute@mustermann.de

1234 5678 9876 5432

Leak auf www.musterfirma.de

Achtung, Ihre E-Mail ute@mustermann.de wurde in einem Leak gefunden. Melden Sie sich so schnell es geht bei musterfirma.de mit der E-Mail-Adresse an und ändern Sie das Passwort. Dann sind Sie auf der sicheren Seite!

Linus Töbke,
Ihr Cyberberater

Cyber Insights: Phishing-Mails mit Corona Bezug

Aktuell werden viele Spam- und Phishing-Mails rund um das Thema Corona verschickt. So geben sich beispielweise Kriminelle als die Weltgesundheitsbehörde (WHO) aus. In der E-Mail ist ein PDF mit praktischen Tipps & Tricks gegen den Corona-Virus angehangen. Tatsächlich handelt es sich leider nicht um gut gemeinte Tipps, sondern um Malware, die bei den Opfern verherende Schäden anrichten kann. Darum sollten Sie aktuell gerade bei E-Mails mit Coronabezug besonders skeptisch sein. Prüfen Sie die E-Mail genau auf Ungereimtheiten, wie schlechtes Deutsch oder einen unseriösen Absender (z.B.: WHO@organist0232.com) und hinterfragen Sie immer, ob der Absender wirklich Sie persönlich anschreiben würde.

Handlungsempfehlung des Monats: Verwenden Sie einen Passwort-Manager

Es heißt immer, dass man für jede Website ein eigenes Passwort verwenden soll, dass dann auch noch schwer zu erraten ist. Doch wie soll man da den Überblick behalten? Genau dafür sind sogenannte Passwort-Manager gemacht. Diese speichern alle Passwörter für jede beliebige Website und können neue, sichere Passwörter generieren. Manche Passwort-Manager füllen sogar die Anmeldedaten auf der entsprechenden Website automatisch aus. Sie brauchen sich nur ein (dafür aber möglichst sicheres) Passwort zu merken, um den Passwort-Manager benutzen zu können.

IHR LOGO

Präsentiert das Meme des Monats:

cysmo PRIVATE Reports

Cyber Report April 2020

cysmo powered by ppi

Alles in Ordnung. Keine Auffälligkeiten.

max@mustermann.de
ute@mustermann.de

1234 5678 9876 5432

Wir konnten in Verbindung mit Ihren Daten keine Auffälligkeiten in Leaks feststellen!

Linus Töbke,
Ihr Cyberberater

Cyber Insights: Phishing-Mails mit Corona Bezug

Aktuell werden viele Spam- und Phishing-Mails rund um das Thema Corona verschickt. So geben sich beispielweise Kriminelle als die Weltgesundheitsbehörde (WHO) aus. In der E-Mail ist ein PDF mit praktischen Tipps & Tricks gegen den Corona-Virus angehangen. Tatsächlich handelt es sich leider nicht um gut gemeinte Tipps, sondern um Malware, die bei den Opfern verherende Schäden anrichten kann. Darum sollten Sie aktuell gerade bei E-Mails mit Coronabezug besonders skeptisch sein. Prüfen Sie die E-Mail genau auf Ungereimtheiten, wie schlechtes Deutsch oder einen unseriösen Absender (z.B.: WHO@organist0232.com) und hinterfragen Sie immer, ob der Absender wirklich Sie persönlich anschreiben würde.

Handlungsempfehlung des Monats: Verwenden Sie einen Passwort-Manager

Es heißt immer, dass man für jede Website ein eigenes Passwort verwenden soll, dass dann auch noch schwer zu erraten ist. Doch wie soll man da den Überblick behalten? Genau dafür sind sogenannte Passwort-Manager gemacht. Diese speichern alle Passwörter für jede beliebige Website und können neue, sichere Passwörter generieren. Manche Passwort-Manager füllen sogar die Anmeldedaten auf der entsprechenden Website automatisch aus. Sie brauchen sich nur ein (dafür aber möglichst sicheres) Passwort zu merken, um den Passwort-Manager benutzen zu können.

IHR LOGO

Präsentiert das Meme des Monats: