

WIE GEHT'S?

PGP oder **GnuPG** gibt's kostenlos im Internet. Nach Download und Installation wird ein so genanntes „Schlüsselpaar“ erzeugt. Die eine Hälfte dient zum Verschlüsseln, die andere zum Entschlüsseln. Die Hälfte zum Verschlüsseln schicken Sie an Freunde und Bekannte, die damit Nachrichten an Sie „verschießen“ können. Nur mit dem Gegenstück, das nur Sie selbst besitzen, kann die Nachricht wieder lesbar gemacht werden. Damit Ihr Gegenüber dann auch sicher sein kann, dass er den echten Schlüssel verwendet, besitzt jeder Schlüssel einen „Fingerprint“ Für die gängigen Mailprogramme wie Outlook Express oder Eudora existieren so genannte Plugins, mit denen sich das Auf- und Zuschließen von E-Mails weitgehend automatisieren lässt.

Eine Schritt-für-Schritt-Anleitung finden Sie auf den Webseiten des Datenschutzzentrums. Dort gibt es auch eine Linksammlung mit interessanten Seiten zum Thema Verschlüsselung.

Denn: Datenschutz ist machbar.

ALSO, WER ES GENAU WISSEN WILL:

www.datenschutzzentrum.de/selbstdatenschutz

www.eposwerbung.de

IMPRESSUM



EUROPÄISCHES VEBRAUCHER- ZENTRUM KIEL

- Willestr. 4-6 Tel.: 0431/9 71 93 50
D-24103 Kiel Fax: 0431/9 71 93 60
- E-Mail: evz@evz.de
<http://www.evz.de>
- **PGP-Schlüssel:** RSA 2048 Bit
Key-ID: 0xC2076B9D, erzeugt am 20.04.1999
- **Fingerprint:**
0947 D920 10B3 4433 8A96 168E F105 32FF



UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ (ULD)

- Holstenstraße 98
D-24103 Kiel
- Tel.: 0431/9 88 – 1247
Fax: 0431/9 88 – 1223
- E-Mail: mail@datenschutzzentrum.de
<http://www.datenschutzzentrum.de>
- **PGP-Schlüssel:** RSA 2048 Bit
Key-ID: 0x8BFDD679, erzeugt am 11.07.97
- **Fingerprint:**
042D 0B0E 6D4F F4D3 FB5D 1B6A 318C B401

SAFER SURFEN!

E-MAIL FÜR DICH

NICHT FÜR JEDEN

CLEVER. VERSCHLÜSSELT. MAILEN.

PGP

E-Mail-Verschlüsselung ?

Ich habe doch gar nichts zu verbergen !
Oder ?



UND WAS HABEN SIE SO IN DER MAILBOX?

Ganz gleich, wie persönlich Ihre elektronische Post ist – sie hat auf dem Weg zu Ihnen bereits viele Stationen passiert: z.B. Mailserver, auf denen sie nach Belieben verändert werden könnte. Böswillige Zeitgenossen haben die Möglichkeit, vollkommen andere Nachrichten daraus zu basteln. Und woher wissen Sie eigentlich, dass der Absender stimmt? Ganz zu schweigen von den Leuten, die schon mal die Nase in Ihre Mail gesteckt haben ...

E-MAIL FÜR DICH — NICHT FÜR JEDEN

„... ich weiß nicht, wie es weitergehen soll ...“
„... ich fürchte, die Diagnose ist eindeutig ...“
„... Hallo Schatz, alles Liebe aus ...“
„... aber behalt' es bitte für dich ...“
„... meine Bankverbindung lautet ...“
„... beantrage ich hiermit die Aufnahme ...“
„... einfach gefeuert!. Kannst du dir das vorstellen?“
„... die offene Rechnung vom 12.09. ...“
„... für drei Wochen im Urlaub. Meine Wohnung ...“
„... und dieser Typ, mit dem sie auf der Party ...“
„... mit dem Personalrat sprechen, ob er vielleicht ...“
„... müssen wir Ihnen leider mitteilen ...“
„... Vielen Dank für das Abendessen gestern ...“
„... aber behalt' es bitte für dich ...“
„... denk' positiv. So eine Krankheit muss nicht ...“
„... ist so komisch. Unsere Beziehung ist irgendwie ...“

Die elektronische Post ist schnell, bequem und kostenlos. Genauso einfach können Sie Ihre E-Mails verschlüsseln. Damit nicht jeder liest, was Sie denken.

Dabei helfen Ihnen die Programme **PGP** und **GnuPG**, und natürlich das Unabhängige Landeszentrum für Datenschutz (ULD). Mit **PGP** und **GnuPG** verschlüsseln Sie Ihre E-Mails so, dass nur der richtige Empfänger sie lesen kann. Einzige Voraussetzung: Ihr Gegenüber verwendet ebenfalls eines der beiden Programme – und immer mehr Menschen tun dies inzwischen. Dann können Sie Nachrichten mit einem Mausklick verschlüsseln und ebenso einfach wieder lesbar machen. An dieser Verschlüsselung beißt sich jeder Lauscher die Zähne aus. Egal ob neugierige Kollegen, böswillige Hacker oder staatliche Überwachungsstellen: Mit **PGP** und **GnuPG** steht Ihnen eine starke Verschlüsselung zur Verfügung, gegen die selbst die größten Computer machtlos sind.

PGP

