Bester Schutz vor Spam und Pishing mit ESET

Spam-Mails sind nicht nur störend, sondern auch sehr gefährlich. Rund 80 Prozent der gesamten E-Mail-Kommunikation besteht aus solchen Nachrichten. Für Cyberkriminelle sind diese der effektivste Verteilungskanal für Malware und ein Mittel, um an persönliche Daten von Internetnutzern zu gelangen. Die finanziellen Schäden sind enorm. Daher ist es wichtig, eine effektive Sicherheitslösung zu verwenden. ESET Internet Security und ESET Smart Security Premium bieten einen umfassenden Schutz gegen Spam und Phishing.

Was ist der Unterschied zwischen Spam und Phishing?

Spam steht als Sammelbegriff für alle Formen von massenhaft verschickten und unerwünschten E-Mails. Vom Prinzip her ähneln sie Werbebroschüren im Postkasten, jedoch ist der potentielle Schaden, den sie anrichten können, deutlich höher. Cyberkriminelle überschwemmen Postfächer mit Spam-Mails, damit sie so die Öffnungsraten steigern und sich finanziell bereichern können. Diese Nachrichten werden auch genutzt, um Schadprogramme zu verbreiten. Sehr beliebt sind beispielsweise fingierte Rechnungen, die als PDF- oder Word-Anhang verschickt werden.

Phishing ist auch ein Teil von Spam. Der Unterschied ist, dass Betrüger und Kriminelle mit diesen E-Mails nach Passwörtern und persönlichen Informationen fischen. In den meisten Fällen kommen diese Nachrichten vermeintlich von einer seriösen Bank, einem beliebten Internetanbieter wie Amazon oder anderen bekannten Dienstleistern wie DHL. Darin werden die Empfänger aufgefordert, aufgrund eines aufgetretenen technischen Problems oder Updates ihre persönlichen Daten erneut einzugeben: Als Vorwand für die Bestätigung von Kontoinformationen wird etwa der baldige Ablauf einer Kreditkarte genannt. Sowohl die Phishing-Mail als auch die Website, auf die ein Link im Text verweist, sind dabei zumeist täuschend echt nachgeahmt. Arglose Empfänger lassen sich so leichter dazu verleiten, auf einen Link zu klicken. Auch in sozialen Netzwerken kommt es zu Phishing. Hier können Links in Postings zum Beispiel für vermeintliche Gewinnspiele zu gefälschten Webseiten führen.

ESET Spam-Schutz prüft unerwünschte Nachrichten

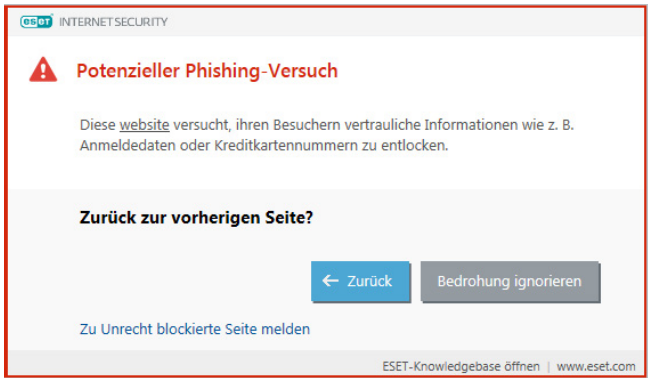
Mit dem ESET Spam-Schutz werden unerwünschte Nachrichten direkt aussortiert. Ein zentrales Prinzip beim ESET Spam-Schutz ist die Möglichkeit, unerwünschte E-Mails über eine Positiv- bzw. eine Negativliste abzugleichen. In der Positivliste werden vertrauenswürdige E-Mail-Adressen, in der Negativliste Spam-Adressen vorab definiert. Alle Adressen in Ihrer Kontaktliste sowie alle vom Benutzer als "sicher" eingestuften Adressen werden automatisch der Positivliste hinzugefügt.

Die primäre Methode zur Spam-Erkennung ist die Prüfung der E-Mail-Eigenschaften. Empfangene Nachrichten werden anhand grundlegender Spam-Kriterien und mithilfe spezifischer Methoden (Nachrichtendefinitionen, statistische Heuristik, Erkennung von Algorithmen usw.) untersucht. Der sich daraus ergebende Indexwert entscheidet darüber, ob eine Nachricht als Spam eingestuft wird oder nicht.

Die ESET Sicherheitslösungen bieten den Spam-Schutz für die E-Mail-Programme Microsoft Outlook, Outlook Express, Windows Mail und Windows Live Mail.

Wie funktioniert Anti-Phishing bei ESET?

ESET Internet Security und ESET Smart Security Premium bieten Anwendern einen Phishing Schutz, der es erlaubt, Webseiten mit Phishing-Inhalt zu filtern.



ESET schützt vor dem Besuch gefährlicher Webseiten.

Die Anti-Phishing-Technologie von ESET schützt Online-Nutzer vor Angriffen auf Passwörter, Bankdaten und andere sensible Informationen durch gefälschte Internetseiten, die sich als legitime Websites tarnen. Versucht der Computer auf eine URL zuzugreifen, vergleicht ESET sie mit einer regelmäßig aktualisierten Datenbank bekannter Phishing-Sites. Wird eine Übereinstimmung gefunden, wird die Verbindung zur URL beendet und eine Warnmeldung angezeigt. Anwender haben stets die Möglichkeit, die URL auf eigene Gefahr zu nutzen.

TIPPS

zum Schutz vor Spam- und Phishing-Mails

- **Im Zweifel die E-Mail löschen**: Nachrichten von unbekannten Absendern oder E-Mails mit seltsamen Inhalten sollten im Zweifel gelöscht werden.
- **Nicht auf enthaltene Links klicken**: Gelangt doch einmal eine Spam-Mail durch die Filter ins Postfach, sollte nicht auf Links geklickt und auf gar keinen Fall persönliche Informationen wie Kreditkartendaten preisgeben werden.
- **Keine Anhänge öffnen**: Häufig werden Anhänge in Spam-Mails als vermeintliche Rechnungen im PDF-, Exe- oder Word-Format getarnt. Diese sollten unter keinen Umständen geöffnet werden. In den meisten Fällen lauern hier Schadprogramme, die so auf das System gelangen.
- **Nicht antworten**: Internetnutzer sollten niemals auf Spam- und Phishing-Mails antworten. Auch vermeintliche Abmelde-Optionen sollten nicht genutzt werden. Die Rückmeldungen sind für Kriminelle eine Bestätigung, dass die Adresse aktiv genutzt wird.
- **Zweit-Adresse anlegen**: Die private E-Mail-Adresse sollte nur in Ausnahmefällen herausgegeben werden. Für Bestellungen in Online-Shops oder Anmeldungen auf Portalen ist es besser, sich ein zweites Postfach zuzulegen. Wer über diese E-Mail viel Spam bekommt, kann einfach zu einer neuen wechseln.
- **Sicherheitslösung einsetzen**: Anwender sollten eine Sicherheitslösung einsetzen, die neben einem zuverlässigen Schutz vor Schadprogrammen auch einen umfassenden Spam- und Phishing-Schutz bietet.
- **Updates einspielen**: Anwender sollten bereitgestellte Updates für das Betriebssystem, die installierte Software und auch Hardware umgehend einspielen. Empfehlenswert ist es die automatische Updatefunktion, wenn verfügbar, zu aktivieren.