



## Vermeehrt stellen wir den Versand von Phishing E-Mails fest. Wie schützen Sie sich vor Phishing Mails?

Phishing-Mails sind betrügerische Nachrichten, die oft versuchen, Sie dazu zu bringen, persönliche oder geschäftliche Informationen preiszugeben. Phishing-E-Mails können für Hacker der Schlüssel sein, um auf Ihre Privat- oder Unternehmenskonten zuzugreifen und diese zu kontrollieren. Dies führt wiederum zu weiteren Betrügereien oder Sicherheitsverletzungen. Ein häufiges Merkmal ist, dass sich hinter dem angezeigten Absender eine andere E-Mail-Adresse verbirgt. Hier sind einige Schritte, um Phishing-Mails zu identifizieren:

### 1. Überprüfen der Absender E-Mail-Adresse

Wenn Sie Ihre E-Mails über einen Browser abrufen, können Sie den Quelltext der HTML-Mail einsehen. In den meisten E-Mail-Programmen genügt es, den Mauszeiger über die Absenderzeile zu bewegen, ohne darauf zu klicken. So können Sie feststellen, ob eine andere Adresse hinterlegt ist.

Achten Sie bitte auf die richtige Schreibweise des Absender. Die European Pallet Association e.V. nutzt ausschließlich die folgende E-Mail-Kombination [Vorname.Nachname@epal-pallets.org](mailto:Vorname.Nachname@epal-pallets.org). Wir fordern Sie niemals zur Eingabe vertraulicher Daten per E-Mail auf.

Anfragen und Änderungen von sensiblen Unternehmensdaten, wie zum Beispiel von Bankdaten wird EPAL über Ihren sicheren Bereich in [My EPAL](#) bestätigen!

### 2. Achten Sie auf folgende Warnsignale:

- **Gefälschte E-Mail-Absender-Adresse:** Überprüfen Sie, ob die angegebene Adresse mit der offiziellen E-Mail Adresse der EPAL übereinstimmt.
- **Dringender Handlungsbedarf:** Phishing-Mails versuchen oft, Druck auszuüben, indem sie behaupten, dass sofortige Maßnahmen erforderlich sind.
- **Rechtschreib- und Grammatikfehler:** Achten Sie auf fehlerhafte Sprache oder unprofessionelle Formulierungen.
- **Links zu gefälschten Webseiten:** Sehen Sie sich die Links genau an, bevor Sie daraufklicken. Oft führen sie zu gefälschten Seiten. Diese Websites sind täuschend echt und sehen aus wie die offiziellen Webseiten bekannter Unternehmen. Sobald der Nutzer seine Daten eingibt, werden diese an die Angreifer übermittelt.
- **Abfrage vertraulicher Daten:** Seien Sie vorsichtig, wenn Sie aufgefordert werden, persönliche Informationen wie Passwörter oder Kontodaten einzugeben.
- **Vorsicht bei Anhängen:** Prüfen sie zuerst die E-Mail, bevor Sie einen Anhang öffnen.

Haben Sie eine Eingangs-E-Mail als Betrugsversuch identifiziert, klicken Sie nicht links und öffnen Sie keine Anhänge. Klicken Sie, wenn möglich mit der rechten Maustaste auf die Mail, im Anschluss auf „Sperrern“ und bestätigen mit „Absender sperren“ und löschen Sie die E-Mail.

Indem Sie diese Hinweise beachten, können Sie sich besser vor Phishing-Angriffen schützen. Sollten Sie bei einer E-Mail Zweifel haben, ob es sich um eine echte E-Mail der European Pallet Association e.V. oder um einen Betrugsversuch handelt, wenden Sie sich bitte gerne an uns. Leiten Sie uns dafür eine vollständige E-Mail (inkl. Adressdaten) an [info@epal-pallets.org](mailto:info@epal-pallets.org) weiter.

Wir unterstützen Sie bei der Prüfung der E-Mail und melden uns schnellstmöglich bei Ihnen.