# zvdh-kompakt

# 04/2025

## Phishing, Smishing & Co. – Cybergefahren für Handwerksbetriebe

**Köln, 31. Januar 2025**

Das Handwerk setzt zunehmend auf digitale Lösungen, doch genau das macht Handwerksbetriebe auch zu attraktiven Zielen für Cyberkriminelle. Der aktuelle Pishing-Versuch, der gerade eine Vielzahl unserer Betriebe erreichte, hat dies erneut gezeigt. Im aktuellen Fall werden die Empfänger aufgefordert, sich per E-Mail bei der SOKA-DACH zu registrieren und Unternehmensdaten preiszugeben. Die Mailadresse ist geschickt angelegt und klingt auf den ersten Blick plausibel: "betriebserfassung@soka-dach.live" oder "arbeitgeber@soka-dach.online".

### Phishing: Die digitale Falle im E-Mail-Postfach

Beim Phishing (von „fishing“ = angeln) versuchen Betrüger, durch gefälschte E-Mails an sensible Daten wie Passwörter oder Bankinformationen zu gelangen. Die Mails wirken täuschend echt und scheinen oft von bekannten Unternehmen oder sogar Geschäftspartnern zu stammen.
Typische Merkmale von Phishing-Mails:

- Dringlichkeit („Ihr Konto wird gesperrt, wenn Sie nicht sofort handeln!“)
- Gefälschte Absenderadresse, die einem bekannten Unternehmen ähnelt
- Links zu täuschend echten Webseiten
- Aufforderung zur Eingabe von Passwörtern oder Bankdaten

Schutzmaßnahme: Keine Links oder Anhänge in verdächtigen E-Mails anklicken! Im Zweifel beim Absender nachfragen.

### Smishing: Gefährliche SMS & WhatsApp

Smishing ist eine Mischung aus „SMS“ und „Phishing“. Hierbei werden betrügerische Nachrichten per SMS oder WhatsApp versendet.
Typische Beispiele:

- „Ihr Paket konnte nicht zugestellt werden. Klicken Sie hier zur Bestätigung: [gefährlicher Link]“
- „Ihr Konto wurde gesperrt! Rufen Sie sofort diese Nummer an.“

Schutzmaßnahme: Keine Links in unerwarteten SMS oder Messenger-Nachrichten anklicken!

### Ransomware: Erpressung durch Verschlüsselung

Hier handelt es sich um Schadsoftware, die nach dem Öffnen einer infizierten Datei alle Daten auf dem Computer verschlüsselt. Erst gegen eine hohe Lösegeldzahlung wird eine Entschlüsselung versprochen – oft ohne Garantie, dass die Daten wirklich freigegeben werden.
Typische Infektionswege:
- Anhänge in gefälschten E-Mails
- Downloads von unseriösen Webseiten
- USB-Sticks unbekannter Herkunft

Schutzmaßnahme: Regelmäßige Datensicherungen auf einem externen Speicher durchführen!

### Wenn Betrüger sich als Chef ausgeben

Hierbei gibt sich ein Betrüger per E-Mail als Geschäftsführer oder Chef aus und fordert Mitarbeitende auf, dringend hohe Geldbeträge auf ein bestimmtes Konto zu überweisen (CEO-Fraud).
Beispiel:
- E-Mail an die Buchhaltung: „Überweisen Sie dringend 20.000 € auf dieses Konto. Ich bin in einer wichtigen Besprechung und nicht erreichbar.“

Schutzmaßnahme: Bei ungewöhnlichen Zahlungsaufforderungen immer telefonisch rückversichern!

### Social Engineering: Psychologische Manipulation

Cyberkriminelle versuchen, durch persönliche Anrufe oder E-Mails an vertrauliche Informationen zu gelangen. Sie geben sich als IT-Dienstleister oder Handwerkskammer aus und fragen nach Passwörtern oder Betriebsdaten.
Typische Tricks:
- „Ich bin von Ihrer Bank, wir müssen Ihr Passwort zurücksetzen. Bitte nennen Sie es mir.“
- „Ich bin ein neuer Mitarbeiter der IT-Abteilung. Können Sie mir Zugang zu Ihrem System geben?“

**Wichtige Infos**: Themenseite Cybersicherheit

Herausgeber: Zentralverband des Deutschen Dachdeckerhandwerks e.V., Fritz-Reuter-Straße 1, 50968 Köln
☎ 0221-398038-0 0221-398038-99 E-Mail zvdh@dachdecker.de // Internet www.dachdecker.de
ZVDH auf Facebook // verantwortlich: Claudia Büttner