99109014014000

Modul	Sachverhalt
Leistungsschlüssel	99109014014000
Leistungsbezeichnung I	
Leistungsbezeichnung II	Phishing-Mail; Meldung
Typisierung	2/3 - Bund: Regelung (2 oder 3), Land/Kommune: Vollzug
Quellredaktion	Bayern
Freigabestatus Katalog	unbestimmter Freigabestatus
Freigabestatus Bibliothek	unbestimmter Freigabestatus
Begriffe im Kontext	
Leistungstyp	
Leistungsgruppierung	
Verrichtungskennung	
SDG-Informationsbereich	
Lagen Portalverbund	
Einheitlicher Ansprechpartner	
Fachlich freigegeben am	11.06.2025

Modul	Sachverhalt
Fachlich freigegen durch	Bayerisches Staatsministerium für Umwelt und Verbraucherschutz
Handlungsgrundlage	
Teaser	Beim so genannten "Phishing" handelt es sich um eine Form des Online-Trickbetruges. Meist sind es E-Mails, die dazu verleiten sollen, wichtige Informationen preiszugeben. Sie können den Erhalt einer Phishing-Mail melden.
Volltext	Meist sind es E-Mails, die - als offizielle Schreiben getarnt - den Internetnutzer verleiten sollen, wichtige Informationen wie Passwörter und Geheimzahlen preiszugeben. Aber auch Fake-SMS werden häufig verschickt. Seriöse Dienstleister fragen niemals per E-Mail, Telefon oder SMS vertrauliche Kundendaten ab. Falls Sie eine Mail erhalten, in der Sie aufgefordert werden, geheime, persönliche Daten einzugeben, sollten Sie darauf weder antworten, noch Anhänge oder enthaltene Links öffnen. Die Bezeichnung Phishing leitet sich vom Fischen (engl. fishing) nach persönlichen Daten ab. Die Ersetzung von F durch Ph ergibt sich dabei aus der Kombination der Worte password harvesting (engl. für Passwort-Ernte). Die Betrüger möchten also möglichst viele Passwörter und Zugangsdaten ernten. Phishing-Angriffsziele sind vornehmlich Zugangsdaten für Bankenportale, Bezahlsysteme wie z. B. PayPal, Online-Shops oder Internet-Auktionshäuser. Mit den gestohlenen Zugangsdaten kann ein großer Schaden verursacht werden, vor allem natürlich Vermögensschäden, aber auch die Installation von Schadsoftware oder Rufschädigung durch die Übernahme der Identität des Opfers. Die neuesten Warnungen gibt es im Phishing-Radar der Verbraucherzentralen. Der Warnmelder informiert über aktuelle Bedrohungen. In einem angeschlossenen Forum haben Sie die Möglichkeit, sich über die aktuell im Umlauf befindlichen Phishing-E-Mails zu den einzelnen Anbietern zu informieren.

Modul	Sachverhalt
Erforderliche Unterlagen	
Voraussetzungen	Ein Internet-Betrüger hat unter dem Anschein eines bekannten Unternehmens oder einer Institution versucht ein Passwort, eine Kontonummer, Telefonnummer oder andere persönliche Daten von Ihnen "abzufischen".
Kosten	keine Die Internetanwendung "Phishing-Radar" ist ein kostenloser Service.
Verfahrensablauf	Wer Opfer einer Phishing-Mail geworden ist, • sollte unverzüglich den betreffenden Dienstanbieter informieren und Strafanzeige erstatten. • sollte die gefälschte E-Mail speichern. Diese könnte als Beweismittel in einem Strafverfahren dienen. • sollte, sofern noch möglich, seine Passwörter unverzüglich ändern, damit die gestohlenen Originalpasswörter unbrauchbar werden. • sollte das Smartphone im Falle einer betrügerischen SMS in den Flugmodus schalten, die schädliche App deinstallieren oder sogar das Geräts in den Auslieferungszustand zurücksetzen und den Mobilfunkanbieter informieren. Sie können Phishing-Mails direkt an die Adresse phishing@verbraucherzentrale.nrw zur Auswertung durch die Verbraucherschützer weiterleiten. Benachrichtigen Sie möglichst auch die Firmen und Institutionen, unter deren Namen die "Datenfischer" agieren. Damit helfen Sie den Unternehmen und Einrichtungen, gegen die Betrüger vorzugehen. Wenn Sie merken, dass Sie auf eine Phishing-Mail hereingefallen sind, sollten Sie das zur Anzeige bei der nächsten Polizeidienststelle bringen.
Bearbeitungsdauer	
Frist	keine
weiterführende Informationen	https://www.verbraucherzentrale-bayern.de/wissen/digitale-welt/phishingradar https://www.verbraucherzentrale-bayern.de/wissen/di

Modul	Sachverhalt
	gitale-welt/phishingradar
Hinweise	Wie kann man sich schützen? • Banken, Versicherungen und auch andere Dienstanbieter fordern von ihren Kunden nie die Zusendung von Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per E-Mail, per SMS oder am Telefon. • Darum gilt: Geben Sie niemals sicherheitsrelevante Daten per E-Mail, SMS oder am Telefon weiter. • Außerdem sollte man niemals Links aus einer unaufgefordert zugesandten E-Mail oder aus einer SMS unbekannter Herkunft aufrufen. Lassen Sie sich die E-Mail ohne HTML anzeigen. URLs und E-Mail-Absenderadressen können gefälscht werden und sind generell nicht vertrauenswürdig. • Beim Onlinebanking sollte man das gewünschte Ziel immer von Hand in die Adresszeile des Browsers eingeben oder im Browser gespeicherte Lesezeichen verwenden, die man selbst sorgfältig angelegt hat. Bevor sicherheitsrelevante Daten angegeben werden, sollte man sich vergewissern, dass es sich um die Original-Webseite handelt. • Generell gilt: Wenn man unaufgefordert in sicherheitsrelevanten Bereichen angesprochen wird, sollte man von vornherein misstrauisch sein. Es ist immer besser, zunächst beim Dienstanbieter nachzufragen, wenn man unsicher ist.
Rechtsbehelf	
Kurztext	
Ansprechpunkt	
Zuständige Stelle	
Formulare	
Ursprungsportal	BayernPortal, BayernPortal