99109014014000

Modul	Sachverhalt
Leistungsschlüssel	99109014014000
Leistungsbezeichnung I	
Leistungsbezeichnung II	Phishing mail; message
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 (Bavarian State Ministry of the Environment and Consumer Protection)
Handlungsgrundlage	
Teaser	Phishing" is a form of online fraud. It usually involves e-mails that are designed to trick you into revealing important information. You can report the receipt of a phishing e-mail.
Volltext	These are usually e-mails disguised as official correspondence designed to trick Internet users into disclosing important information such as passwords and PINs. Fake text messages are also frequently sent. Reputable service providers never ask for confidential customer data by e-mail, telephone or text message. If you receive an e-mail asking you to enter secret personal data, you should not reply to it or open any attachments or links contained in it. The term phishing is derived from fishing for personal data. The substitution of F for Ph results from the combination of the words password harvesting. In other words, the fraudsters want to harvest as many passwords and access data as possible. Phishing attack targets are primarily access data for banking portals, payment systems such as PayPal, online stores or Internet auction houses. The stolen access data can cause a great deal of damage, above all financial loss, of course, but also the installation of malware or damage to reputation by assuming the victim's identity. The latest warnings can be found in the phishing radar of the consumer advice centers. The alert informs you about current threats. In a connected forum, you have the opportunity to find out about the phishing e-mails currently in circulation from the individual providers.
Erforderliche Unterlagen	
Voraussetzungen	An Internet fraudster has tried to "fish" a password, account number, telephone number or other personal

Modul	Sachverhalt
	data from you under the guise of a well-known company or institution.
Kosten	none The Internet application "Phishing Radar" is a free service.
Verfahrensablauf	Anyone who has fallen victim to a phishing e-mail • should immediately inform the service provider concerned and file a criminal complaint. • should save the forged e-mail. This could serve as evidence in criminal proceedings. • should, if still possible, change their passwords immediately so that the stolen original passwords become unusable. • should switch the smartphone to flight mode in the event of a fraudulent text message, uninstall the malicious app or even reset the device to the factory settings and inform the mobile phone provider. You can forward phishing emails directly to phishing@verbraucherzentrale.nrw for evaluation by consumer protection agencies. If possible, also notify the companies and institutions under whose name the "data fishers" are operating. This will help the companies and institutions to take action against the fraudsters. If you notice that you have been taken in by a phishing e-mail, you should report it to the nearest police station.
Bearbeitungsdauer	
Frist	none
weiterführende Informationen	https://www.verbraucherzentrale-bayern.de/wissen/digitale-welt/phishingradar https://www.verbraucherzentrale-bayern.de/wissen/digitale-welt/phishingradar
Hinweise	How can you protect yourself? • Banks, insurance companies and other service providers never ask their customers to send them

Modul	Sachverhalt
	credit card numbers, PINs, TANs or other access data by e-mail, text message or telephone. • The following therefore applies: Never pass on security-relevant data by e-mail, text message or over the phone. • You should also never open links from an unsolicited e-mail or text message of unknown origin. Display the e-mail without HTML. URLs and e-mail sender addresses can be forged and are generally not trustworthy. • When banking online, you should always enter the desired destination manually in the address line of the browser or use bookmarks saved in the browser that you have carefully created yourself. Before entering security-relevant data, you should make sure that it is the original website. • As a general rule, if you are approached unsolicited in security-relevant areas, you should be suspicious from the outset. It is always better to ask the service provider first if you are unsure.
Rechtsbehelf	
Kurztext	
Ansprechpunkt	
Zuständige Stelle	
Formulare	
Ursprungsportal	BayernPortal, BayernPortal