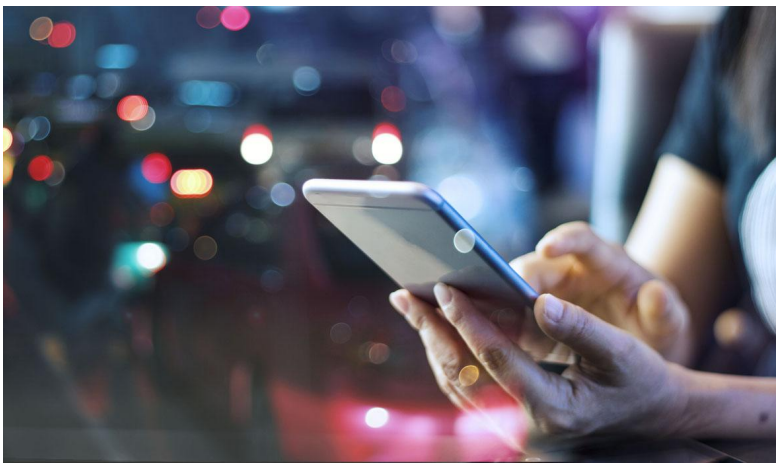
verbraucherzentrale
Hamburg

Achtung, Phishing – so handeln Sie richtig!

Tag für Tag landen gefährliche Nachrichten in den digitalen Postfächern vieler Verbraucherinnen und Verbraucher – sogenannte Phishing-Mails. Vermeintliche Absender sind oft bekannte Unternehmen wie Banken, Versicherungen oder Krankenkassen. Doch nun nutzen Betrüger sogar den Weg per Post. So handeln Sie richtig.



DAS WICHTIGSTE IN KÜRZE

1. Betrügerische E-Mails und Nachrichten sehen oft täuschend echt aus. Mittlerweile werden sie nicht nur digital, sondern auch als Schreiben mit der Briefpost verschickt.

2. Bei fragwürdigen Mitteilungen, empfiehlt es sich den Anbieter direkt zu kontaktieren und nachzufragen, ob die Nachricht echt ist. Die richtigen Kontaktdaten der Unternehmen sind über deren Internetseite abrufbar.
3. Um Betrugsversuchen vorzubeugen, ist es wichtig, keine Anhänge zu öffnen, nicht auf Links zu klicken und keine QR-Codes zu scannen.
4. **Kostenloser Vortrag in Hamburg: „Abzocke im Alter - So schützen Sie sich vor Betrug“** Jetzt anmelden

Stand: 13.08.2024

Phishing ist ein Kunstwort, das sich aus „password” und „fishing” zusammen setzt. Es handelt sich um eine besondere Form unverlangt zugesandter Nachrichten, mit denen Betrüger versuchen, geheime Zugangsdaten abzufragen. Dabei geht es um Ihr Geld. Wie beim Fischen hoffen die Täter, dass ihnen einige arglose Verbraucherinnen und Verbraucher ins Netz gehen. Versteckter Mitreisender dieser Mails oder der SMS ist in vielen Fällen Schadsoftware, über die sensible Nutzerdaten in die Hände von Betrügern gelangen können.

Phishing-Mails oder Smishing-Nachrichten (SMS) sind eine zunehmende Gefahr. Getarnt als Rechnung, Mahnung, Fax, Bestellung oder Mitteilung der eigenen Bank landen sie immer wieder in den digitalen Postfächern oder auf den Mobilfunkgeräten vieler Menschen. Vermeintliche Absender sind oft bekannte Unternehmen wie Amazon, AOK, Paypal oder die Deutsche Telekom. Doch mittlerweile ist sogar echte Briefpost mit beigefügten QR-Codes im Umlauf.

So tappen Sie nicht in die Phishing-Falle

- **Genau prüfen:** Seien Sie auf der Hut und prüfen Sie jede E-Mail oder SMS und ggf. Briefpost, die in Ihrem digitalen Postfach oder echtem Briefkasten landet, genau!
- **„Wahrscheinlichkeits-Check“ machen:** Wie wahrscheinlich ist es, dass diese Unternehmen Ihnen schreibt? Haben Sie überhaupt Vertragsbeziehungen mit der

Firma? Wie nimmt der Absender üblicherweise Kontakt mit Ihnen auf?

- **Keine Anhänge und Links öffnen, keine QR-Codes scannen:** Öffnen Sie keinesfalls die übermittelten Anhänge wie ZIP- oder EXE-Dateien, und klicken Sie nicht auf Links in der Mail oder der SMS, scannen Sie keine QR-Codes! Sollten Sie denken, dass vielleicht doch was dran sein könnte, geben Sie die Internetadresse des Unternehmen direkt über den Browser ein.
- **Nachricht sofort entsorgen:** Löschen Sie die betrügerischen Mails sofort und zwar gänzlich von Ihrem Computer. Entsorgen Sie betrügerische Briefe im Papiermüll!

Auffallend ist, dass Phishing-Nachrichten in der Aufmachung immer professioneller werden. Sie imitieren geschickt den Firmenauftritt derer, für die sie sich ausgeben. Rechtschreibfehler kommen kaum noch vor, sodass die getarnten Schreiben schwerlich als solche zu erkennen sind. Mit den Schreiben, die per Post ins Haus flattern, nehmen die Betrüger wohl vor allem ältere Menschen ins Visier.

Weil die Täter meist im Ausland sitzen, ist es schwierig, der Bedrohung mit Mitteln der Strafverfolgung Herr zu werden. Auch technische Schutzmaßnahmen wie Antiviren-Software und moderne Web-Browser können das Problem lediglich mildern.

GUT ZU WISSEN

Angesichts täglich neuer Betrugsversuche ist es ratsam, sich regelmäßig über aktuelle Phishing-Mails zu informieren. Ihren Posteingang gleichen Sie am besten mit den Hinweisen des Phishing-Radars der Verbraucherzentrale Nordrhein-Westfalen ab.

https://www.vzhh.de/themen/telefon-internet/phishing-mails-spam/achtung-phishing-so-handeln-sie-richtig