

## **Wichtiger Hinweis zu neuer Betrugsmasche mithilfe von Auftragnehmer-/ Auftraggeber Daten!**

### Phishing: TED warnt vor Betrug mit Bekanntmachungsdaten

Per Mail weist TED Vergabestellen nach Veröffentlichung einer EU-Bekanntmachung auf aktuelle Phishing-Fälle hin.

In den verzeichneten Betrugsfällen nutzen Betrüger Informationen über erteilte Aufträge die bspw. auf Plattformen wie TED veröffentlicht werden. Sie nehmen Kontakt mit dem Lieferanten auf, geben sich als Auftraggeber aus und fordern die Zusendung der Rechnung zu dem auf TED veröffentlichten Auftrag an.

Nach Erhalt der Rechnung nehmen die Täter wiederum Kontakt mit dem Auftraggeber auf und geben sich als Lieferant aus. Sie reichen die Rechnung mit abweichenden Bankdaten beim Auftraggeber ein und fordern zur Zahlung auf.

Das Amt für Veröffentlichungen rät daher zu besonderer Vorsicht, besonders wenn man aufgefordert wird, eine Zahlung an einen Lieferanten auf ein unerwartetes Bankkonto zu machen. Wenn man denkt, dass es sich um Betrug handeln könnte, sollte man den Lieferanten direkt über einen bekannten Kommunikationsweg kontaktieren.

Folgend finden Sie die originale Warnmeldung seitens TED sowie die deutsche Übersetzung.

<b>Englisch</b>	<b>Deutsch</b>
<p>*** Important notice ***</p> <p>If you have published or will publish the details of the winners of your procurement procedure on TED, please be aware of the fraud method described below. A number of successful attempts have been reported based on this method or with variations:</p> <ul style="list-style-type: none"> <li>• Fraudsters monitor websites where information about awarded contracts is published, such as TED.</li> <li>• They first contact the supplier. They pretend to be the customer and ask to be forwarded the invoice related to the contract published on TED.</li> <li>• Once they have received the invoice, they contact the customer, pretending to be the supplier. They request that the payment be made to another bank account than the one listed on the real invoice, which will be an account controlled by the fraudsters.</li> </ul>	<p>*** Wichtiger Hinweis ***</p> <p>Wenn Sie die Details der Gewinner Ihres Vergabeverfahrens auf TED veröffentlicht haben oder veröffentlicht werden, beachten Sie bitte die unten beschriebene Betrugsmethode. Es wurde von einer Reihe erfolgreicher Versuche berichtet, die auf dieser Methode oder auf Abwandlungen davon basieren:</p> <ul style="list-style-type: none"> <li>- Die Betrüger überwachen Websites, auf denen Informationen über vergebene Aufträge veröffentlicht werden, wie z. B. TED.</li> <li>- Sie nehmen zunächst Kontakt mit dem Anbieter auf. Sie geben sich als Kunde aus und bitten um die Zusendung der Rechnung für den auf TED veröffentlichten Auftrag.</li> <li>- Sobald sie die Rechnung erhalten haben, setzen sie sich mit dem Kunden in Verbindung, wobei sie vorgeben, der Lieferant zu sein. Sie verlangen, dass die Zahlung auf ein anderes Bankkonto als das auf der echten Rechnung angegebene überwiesen wird, das von den Betrügern kontrolliert wird.</li> </ul>

The key element in the reported cases is the combined use of real contract information and pressure applied by the perpetrators. Given that you are listed on TED as the contact point for your organisation, there is a possibility that you might be targeted by a fraud attempt along the lines described above.

We encourage you to be extra cautious and vigilant, especially if you are asked to make a payment to a supplier using a different bank account than you would have expected.

If you experience something that you suspect could possibly be a fraud attempt, we recommend that you contact the supplier directly to verify that you are paying the right entity. Use an established form of communication with that specific supplier to make sure that you are in contact with the real supplier.

Please inform your collaborators and any other persons who might be exposed to this fraud method. If you find yourself targeted by a fraud attack, please report it to the relevant authorities in your country.

Das Schlüsselement in den gemeldeten Fällen ist die kombinierte Verwendung echter Vertragsinformationen und der von den Tätern ausgeübte Druck.

Da Sie bei TED als Kontaktstelle für Ihre Organisation aufgeführt sind, besteht die Möglichkeit, dass Sie Ziel eines Betrugsversuchs nach dem oben beschriebenen Muster werden.

Wir empfehlen Ihnen, besonders vorsichtig und wachsam zu sein, vor allem, wenn Sie aufgefordert werden, eine Zahlung an einen Lieferanten zu leisten, der ein anderes Bankkonto verwendet, als Sie erwartet hätten. Wenn Sie den Verdacht haben, dass es sich um einen Betrugsversuch handeln könnte, empfehlen wir Ihnen, sich direkt mit dem Lieferanten in Verbindung zu setzen, um sich zu vergewissern, dass Sie an das richtige Unternehmen zahlen.

Verwenden Sie eine etablierte Form der Kommunikation mit dem betreffenden Anbieter, um sicherzustellen, dass Sie mit dem tatsächlichen Anbieter in Kontakt stehen.

Bitte informieren Sie Ihre Mitarbeiter und alle anderen Personen, die von dieser Betrugsmethode betroffen sein könnten. Wenn Sie von einem Betrugsversuch betroffen sind, melden Sie dies bitte den zuständigen Behörden in Ihrem Land.