Die 10 wichtigsten Tipps zur Vermeidung von Phishing-Attacken

	Maßnahmen zum Schutz vor Phishing-Attacken	
Tipp 1	Wenn Sie E-Mails von **Online-Banken, Kreditinstituten** oder anderen Internetdienstleistern bekommen, in denen Sie aufgefordert werden, Ihre geheimen Zugangs- und Kontodaten einzugeben, sollten Sie darauf nicht reagieren und die E-Mails am besten gar nicht erst öffnen. Klicken Sie auf keinen Fall auf die angegebenen Links in den E-Mails. Falls Sie nicht sicher sind, ob nicht doch die Bank der Absender ist, gehen Sie per Browser auf die Homepage des Anbieters, indem Sie die Adresse der Homepage manuell eintragen oder den entsprechenden Eintrag aus Ihrem Bookmark-Verzeichnis wählen. Im Zweifelsfall können Sie auch bei dem jeweiligen Institut nachfragen, was es mit der E-Mail auf sich hat. Banken und andere Dienstleister werden Sie niemals nach geheimen Zugangsdaten wie **PINs, TANs** oder **Passwörtern** fragen.	
Tipp 2	Bei verdächtigen E-Mails können Sie versuchen, den tatsächlichen Absender zu ermitteln, indem Sie den Weg der E-Mail zurückverfolgen. Bei Outlook Express finden Sie diese Option z. B. unter **Datei →Eigenschaften→ Details.**	
Tipp 3	Sensible Daten wie PINs und Passwörter sollten bei sicherheitsrelevanten Vorgängen ausschließlich über gesicherte Verbindungen per **SSL** übertragen werden. Zu erkennen sind diese Verbindungen meist durch ein entsprechendes Symbol in Form eines geschlossenen Vorhängeschlosses in der Statusleiste des Browsers. Durch Anklicken dieses Symbols können Sie weitere Informationen zu dieser Website in Erfahrung bringen. Kontrollieren Sie, ob das **Zertifikat** tatsächlich zum Server des vermeintlichen Absenders passt.	
Tipp 4	Um eine Infektion des Rechners mit **Trojanern** und **Spyware** zu verhindern, sollten Sie beim Download von Dateien aus dem Internet vorsichtig sein. Nach Möglichkeit sollten Downloads nur aus vertrauenswürdigen Quellen erfolgen. Unverlangt zugesandte E-Mail-Anhänge unbekannter Absender sollten niemals ohne vorherige Rückfrage geöffnet werden. Selbst wenn die Mail von einem bekannten Absender stammt, sollten Sie skeptisch bleiben, denn auch hier können im Anhang Schadprogramme enthalten sein.	
Tipp 5	Zum Schutz vor Trojanern und Spyware sollten Sie unbedingt eine aktuelle **Antivirensoftware** nutzen, die mit den jeweils neuesten Virenmustern arbeitet. Zusätzlichen Schutz bieten spezialisierte **Anti-Spyware-Programme**. Allerdings erkennen auch diese Programme längst nicht jedes Schadprogramm, sodass Sie selbst dann vorsichtig bleiben sollten, wenn eine Überprüfung ein sauberes System meldet.	
Tipp 6	Halten Sie Ihr Betriebssystem unbedingt auf dem aktuellen Stand. Bei Windows XP lässt sich dies am einfachsten mit dem sog. **Auto-Update** erledigen, das alle sicherheitsrelevanten Patches und Updates völlig autonom herunterlädt und installiert. Ältere Windows-Versionen können Sie über das **Windows-Update** auch manuell auf den neuesten Stand bringen. Aktualisierungen sind auch für den Browser unerlässlich. Beim **Internet Explorer** genügt dazu das Windows-Update, auch die anderen Browser wie **Firefox** oder **Opera** melden sich inzwischen selbstständig, wenn neue Updates vorhanden sind. Sicherheitslücken können darüber hinaus auch durch andere Programme (Media-Player, Office-Anwendungen etc.) entstehen. Auch diese Anwendungen sollten Sie daher aktualisieren, sobald sicherheitsrelevante Updates angeboten werden.	

V. i. S. d. P.: CDU-Bundesgeschäftsstelle | Klingelhöferstraße 8 | 10785 Berlin
www.cdu.de/kontakt | Stand: April 2018

	Maßnahmen zum Schutz vor Phishing-Attacken	
Tipp 7	Geben Sie die Adressen von Webseiten, auf denen Sie **geheime Zugangsdaten** eingeben müssen, immer per Hand in die Adressleiste ein bzw. rufen Sie diese Seiten über den Eintrag in der Lesezeichenliste auf. Dadurch verringern Sie das Risiko, auf einer nachgemachten bzw. gefälschten Seite zu landen, ganz erheblich.	
Tipp 8	Die neuesten Browser-Versionen bieten einen integrierten Phishing-Schutz, der über **Black- und White-Lists** realisiert wird. Beim Aufruf verdächtiger Seiten erscheint dann ein entsprechender Warnhinweis. Auch die Suchmaschine Google blendet mittlerweile Warnungen ein, wenn eine Fundstelle unter Phishing-Verdacht steht. Allerdings können auch diese Systeme keinen zuverlässigen Schutz bieten, und Sie dürfen sich daher in keinem Fall blind auf die Ergebnisse verlassen. Entsprechende Phishing-Filter sind auch in diverse Browser-Toolbars integriert.	
Tipp 9	Sichern Sie ihren **Browser** weitgehend ab und surfen Sie nur mit hohen Sicherheitseinstellungen. Sofern die Nutzung hierdurch nicht zu sehr eingeschränkt bzw. sogar unmöglich gemacht wird, sollten Sie **Java, JavaScript** und im Internet Explorer auch **Active Scripting** deaktivieren, um die hierüber möglichen Angriffe zu verhindern. Sofern der Browser dies unterstützt, sollten Sie diese Funktionen ausschließlich auf ausgewählten vertrauenswürdigen Seiten erlauben und bei noch unbekannten Seiten zunächst generell verbieten. Die aktuelle Opera-Version bietet etwa derartige Einstellmöglichkeiten, beim Firefox lässt sich etwas Ähnliches über die Erweiterung **NoScript** erreichen.	
Tipp 10	Um der Gefahr von **Phishing-Trojanern** und ähnlichen Spyware-Angriffen zu entgehen, empfehlen mittlerweile sogar renommierte Anbieter von Sicherheitssoftware den Umstieg von Windows auf andere Betriebssysteme. Da die meisten Viren, Würmer, Spyware-Programme, Trojaner und Backdoors ausschließlich auf Windows-Rechner spezialisiert sind, können Sie das Risiko hierdurch tatsächlich minimieren. Ob ein solcher Systemwechsel allerdings praktikabel ist, ist eine ganz andere Frage.	