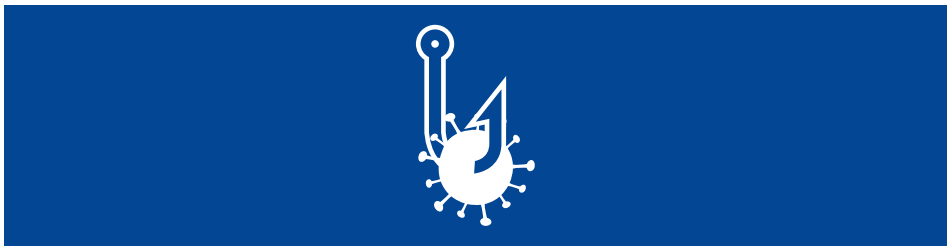
Deutsche Bank
TDI CSO

Wichtige Information
für Geschäftskunden

Warnung vor Cyber-Angriffen in Zusammenhang mit Corona-Pandemie

April 2020

Cyber-Kriminelle nutzen Ängste und Unsicherheit rund um die Ausbreitung von Covid-19 für Angriffe auf die sensiblen Informationen von Unternehmen und ihren Kunden. Mitarbeitende sollten aktuell besonders auf E-Mails, SMS-Nachrichten und Social-Media-Posts achten, die Bezug zur Pandemie nehmen. Es kann sich um Betrugsversuche handeln! Zudem bestehen weitere Cyber-Risiken durch Arbeit im Home Office.



Auf Corona-Phishing achten!

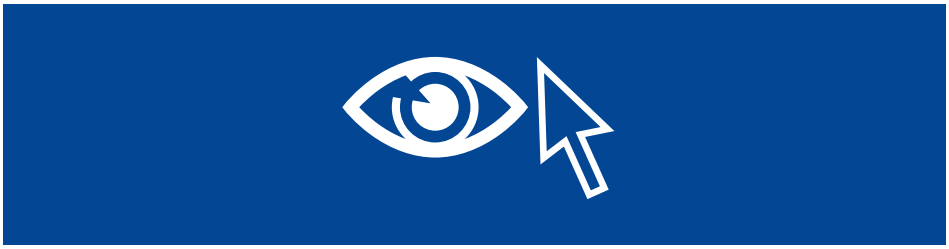
- Die Kriminellen geben sich als seriöse Stellen aus und wählen für die Kontaktaufnahme einen Vorwand mit aktuellem Bezug zur Corona-Pandemie.
- Die betrügerischen Nachrichten sollen dazu verleiten, auf gefälschten Webseiten sensible Informationen wie Zugangsdaten für Online-Konten, Kreditkarten-Informationen und Mobilfunknummern preiszugeben.
- In anderen Fällen sollen Mitarbeitende auf Anhänge oder Links klicken. Dadurch werden ihre Computer oder Smartphones mit Schadprogrammen infiziert, die sensible Daten auslesen oder sie zum Zweck der Erpressung verschlüsseln.
- Sicherheitsexperten beobachten eine Zunahme solcher Phishing-Angriffe per E-Mail, SMS, Anruf, Messenger und Social Media.

Aktuelle Betrugsvarianten

- Im Namen einer seriösen Gesundheits-Organisation wie der WHO, des Centers for Disease Control und Prevention (CDC) oder des Robert Koch

Instituts (RKI) locken Betrüger per E-Mail mit relevanten Informationen zu Covid-19, zum Beispiel zu Hoch-Risiko-Zonen in der Stadt des Empfängers. Um Zugang zu diesen Informationen zu erhalten, sollen die Empfänger auf einen Link klicken oder die Zugangsdaten ihres E-Mail-Accounts preisgeben.

- Kriminelle geben sich als behördliche Stelle aus und kündigen der Geschäftsführung per Telefon, E-Mail oder Textnachricht einen Geldbetrag im Rahmen eines Corona-Soforthilfe-Programms an. Die Empfänger sollen sensible Informationen zu Online-Konten übermitteln, damit der Betrag angewiesen werden könne.
- Im Namen der Personalabteilung des Unternehmens erhalten Mitarbeitende an ihre berufliche E-Mail-Adresse eine gefälschte E-Mail mit einem Link zu einer Management-Leitlinie zur Corona-Krise, die sie lesen sollen.
- Mitarbeitende werden von einem Krankenhaus darüber informiert, angeblich positiv auf Covid-19 getestet worden zu sein und sollen aus diesem Anlass persönliche Informationen übermitteln oder auf einen Anhang klicken.
- Per SMS wird eine App empfohlen, die angeblich positiv auf Covid-19 getestete Menschen in Ihrem Umkreis anzeigt, sobald der Nutzer per Kreditkarte eine geringe Gebühr gezahlt hat.
- Unternehmen werden im Namen einer seriösen Hilfsorganisation in Sachen Corona um eine Spende gebeten. Bei der angegeben Kontoverbindung handelt es sich beispielsweise um einen gefälschten PayPal-Account.
- Mitarbeitende erhalten die betrügerische Nachricht, dass Kosten für stornierte Flüge oder Übernachtungen erstattet würden.
- Nach einer Attacke mit Schadsoftware erscheint im Browser der Mitarbeitende plötzlich eine Webseite, die zum Laden einer bösartigen App mit Empfehlungen zum Schutz gegen das Corona-Virus animiert.
- Eine Fake-News leitet Mitarbeitende auf eine Webseite, auf der schwer erhältliche Produkte wie Desinfektionsmittel, Atemschutzmasken oder Schutzhandschuhe angeboten werden, die jedoch nie geliefert werden.



So schützen Sie sich vor Phishing

Angriffe erkennen und abwehren

- Öffnen Sie keine verdächtige E-Mail, ohne die Adresse des Absenders überprüft zu haben.
- Fahren Sie daher zuerst mit dem Mauspfeil über den Namen des Absenders, damit Ihnen die volle E-Mail-Adresse angezeigt wird.
- Wurde die verdächtige E-Mail im Namen einer seriösen Organisation versendet, so sollten Sie überprüfen, ob diese E-Mail-Adresse die gleiche Zieladresse (Domain) enthält wie die Internetadresse der Organisation.
- So identifizieren Sie die Zieladresse in einer Internet-Adresse (URL): Starten Sie beim „://“ und suchen Sie den nächsten Slash: http(s)://hier-steht-was.Zieladresse.com/hier-steht-auch-was Springen Sie nach links über die Domain-Endung „.com“, „.org“ oder etwa

„.de“ hinweg bis zum nächsten Punkt. Zwischen diesem Punkt und dem nächsten Slash rechts befindet sich die Zieladresse:
http(s)://hier-steht-was.Zieladresse.com/hier-steht-auch-was

- Klicken Sie niemals auf Anhänge oder Links einer E-Mail, wenn Sie sich ihrer Seriosität nicht absolut sicher sein können. Verifizieren Sie Absender und Anlass der Mail beispielsweise per Anruf unter einer Ihnen bereits bekannten Telefonnummer.
- Löschen Sie verdächtige E-Mails umgehend.
- Gefälschte Log-In-Seiten sind vom Original oft nicht zu unterscheiden. Geben Sie daher niemals vertrauliche Informationen wie Kreditkarten-Informationen, Passwörter und andere Zugangsdaten auf Webseiten ein, zu denen Sie der Link einer Nachricht geführt hat, die sie nicht selber zeitnah angefordert haben.
- Bei gewöhnlich versendeten E-Mails können sich die Kommunikations-partner der Identität des anderen sowie der Integrität des Inhalts nicht sicher sein. Senden Sie sensible Informationen daher immer nur als verschlüsselte E-Mail und vertrauen Sie nur E-Mails, die sie verschlüsselt empfangen. Für die Kommunikation mit der Deutschen Bank steht Ihnen dazu db Secure Email zur Verfügung.
- Klicken Sie niemals auf Links in verdächtigen SMS-, Messenger-Nachrichten oder Social-Media-Posts. Auch vertrauenswürdig erscheinende Telefonnummern oder Profile können Fälschungen sein.
- Lassen Sie sich von verdächtigen Anrufern nicht in ein Gespräch verwickeln. Geben Sie niemals sensible Informationen preis. Bitten Sie darum, zurückrufen zu können, falls es sich um einen seriösen Anruf handeln könnte. Nutzen Sie die Zeit, um die Identität des Anrufers und die Plausibilität seines Anliegens zu überprüfen – beispielsweise durch interne Nachfragen oder einen Rückruf bei der Organisation, für die der Anrufer angibt, tätig zu sein.

Vertrauenswürde Informationsquellen

- Seriöse Gesundheits- und Hilfsorganisationen werden Sie niemals per E-Mail dazu auffordern, persönliche Informationen auf Webseiten preiszugeben.
- Informieren Sie sich zu Fragen rund um die Corona-Pandemie auf den Webseiten der Institutionen des Bundes oder der Länder, etwa dem Robert Koch Institut (RKI) oder der Bundeszentrale für gesundheitliche Aufklärung (BZgA).
- Die von Kriminellen aktuell am häufigsten gefälschte Corona-Landkarte ist die der US-amerikanischen Johns-Hopkins-Universität. Die echte Internetadresse lautet https://coronavirus.jhu.edu/map.html

Warnung vor Cyber-Angriffen im Zusammenhang mit Corona-Pandemie

Online Banking

- Die Deutsche Bank sendet Geschäftskunden niemals E-Mails, die Links zum Online Banking enthalten und dazu auffordern, die Nummern von Konten oder Zugangsdaten preiszugeben.
- Nutzen Sie als Geschäftskunde für Abwicklung des Zahlungsverkehrs zur Sicherheit Plattformen der Deutschen Bank wie DB AutoBahn. Dort steht mit dem DB Secure Authenticator eine zwei-Wege-Authentifizierung per Smartphone-App für iOS und Android zur Verfügung.
- Melden Sie sich niemals über einen Ihnen unbekannten Computer für das Online-Banking an.
- Weitere Sicherheitshinweise zum Zahlungsverkehr über die Deutsche Bank finden Sie hier (https://autobahn.db.com/microSite/html/cyber-fraud-prevention.html).

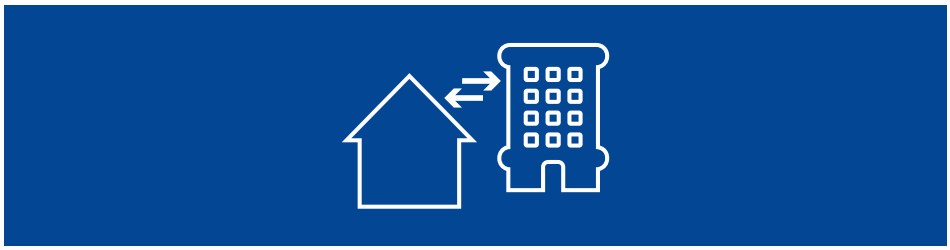
Passwort-Sicherheit

- Verwenden Sie ein und dasselbe Passwort niemals für mehrere Accounts. Andernfalls könnte es Cyber-Kriminellen gelingen, sich per sogenanntem Credential Stuffing mit einem bereits erbeuteten Passwort Zugang zu Ihren weiteren Accounts zu verschaffen. Diese Gefahr ist groß, weil Sie bereits Ihre E-Mail-Adresse als Nutzername für viele Accounts verwenden.
- Geben Sie Passwörter nie an andere weiter.
- Wählen Sie Passwörter mit mindestens 15 Zeichen, bestehend aus Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen. Dann brauchen Sie es nur dann zu wechseln, wenn Sie den Verdacht haben, dass es in falsche Hände geraten sein könnte.
- Speichern Sie Passwörter niemals als digitale Notizen, zum Beispiel im Adressbuch Ihres Smartphones oder in Dokumenten auf Computer, Server oder in Ihrer Cloud.
- Nutzen Sie die Zwei-Wege-Authentifizierung, wo immer Sie Ihnen zur Verfügung steht.

Warnung vor Cyber-Angriffen im Zusammenhang mit Corona-Pandemie

Smartphone-Sicherheit

- Cyber-Kriminelle versuchen, über infizierte Apps Zugangsdaten von Ihrem Smartphone zu erbeuten. Sie bedrohen damit beispielsweise die Sicherheit der Zwei-Wege-Authentifizierung.
- Laden Sie Apps für Smartphone und Tablet daher immer nur aus seriösen Quellen wie dem Google Play Store oder dem Apple App Store.
- Grenzen Sie die Zugriffsrechte Ihrer Apps ein. Erlauben Sie einer App nicht, auf SMS-Nachrichten zuzugreifen.
- Halten Sie das Betriebssystem Ihres Smartphones sowie Apps immer auf dem neusten Stand, weil Updates Sicherheitslücken schließen.
- Achten Sie auf Anzeichen, die für eine Infektion Ihres Smartphones mit Schadsoftware sprechen: Das Gerät reagiert langsam, der Akku wird schnell leer, der Speicher ist plötzlich voll, Apps erscheinen oder verschwinden ohne Ihr Zutun.



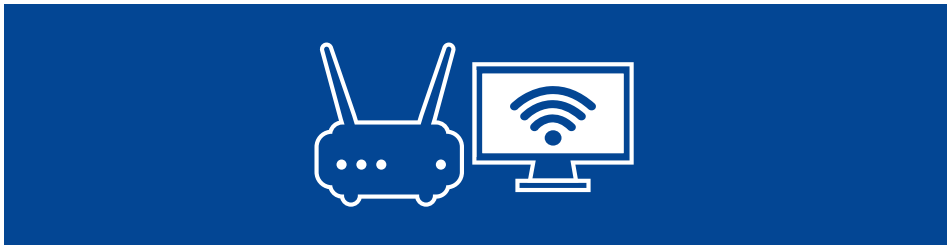
Risiken durch Split Operation und Home Office

- Zum Schutz gegen eine Covid-19-Infektion arbeiten Mitarbeitende derzeit vielfach von Zuhause aus. Damit besteht das Risiko, dass bestimmte technische und organisatorische Maßnahmen des Unternehmens zum Schutz sensibler Informationen nicht greifen.
- Vorsichtsmaßnahmen wie Split Operation und Quarantäne verändern erheblich gewohnte Arbeitsabläufe, Zuständigkeiten und Kommunikationswege. Für Cyber-Kriminelle bieten sich dadurch neue Angriffspunkte – besonders durch Social Engineering.
- Im häuslichen Umfeld können sensible Informationen des Unternehmens zudem durch Mithören, Blicke auf Bildschirme oder Zugriff auf Dokumente unbefugten Personen zugänglich werden. Telefonate und Gespräche könnten über vernetzte Lautsprecher wie Amazon Alexa, Google Home oder Facebook Portal im Fall einer Sicherheitslücke offengelegt werden.
- Das Management sollte auf diese Risiken zeitnah reagieren. Technische Maßnahmen wie die Bereitstellung von VPN-Verbindungen, Regeln und Vorkehrungen für die Nutzung privater Geräte zu geschäftlichen Zwecken sowie die Sensibilisierung der Mitarbeitende für die besonderen Bedrohungen im Home Office in Verbindung mit der aktuellen Corona-Pandemie sind von höchster Wichtigkeit.

Warnung vor Cyber-Angriffen im Zusammenhang mit Corona-Pandemie

Aktuelle Fälle von Social Engineering

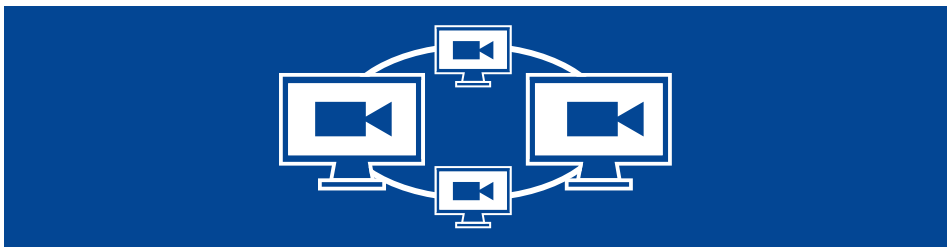
- Kriminelle sammeln per Anruf, Online-Recherche und in Sozialen Medien Informationen über Mitarbeitende, Kunden und Lieferanten, um geeignete Zielpersonen für Cyber-Angriffe zu identifizierten. Auf diese Weise kann es ihnen gelingen, Spear-Phishing-Angriffe auf exponierte Personen des Unternehmens auszuführen, interne Geschäftsprozesse zu manipulieren und Zahlungen auf betrügerische Konten zu lenken.
- Betrüger nutzen aktuell veränderte Vertretungsregelungen in Unternehmen für eine neue Variante des Chef-Betrugs. Sie geben sich per E-Mail beispielsweise einem neu ernannten Vertreter gegenüber als ein Mitarbeitende des Unternehmens aus, der angeblich von der Geschäftsführung zur Freigabe einer eilig zu veranlassenden Zahlungen bevollmächtigt sei.
- Kriminelle treten als Dienstleister oder Lieferanten auf und stellen plausibel erscheinende Rechnungen mit Angabe eines betrügerischen Kontos.
- Ein Betrüger könnte sich als Mitarbeitende der Hausbank eines Unternehmens ausgeben und in Zusammenhang mit einem beantragten Corona-Überbrückungskredit einem Mitarbeitende des Rechnungswesens per E-Mail dazu auffordern, Zugangsdaten für das Online-Banking des Unternehmens auf einer gefälschten Webseite einzugeben. Die erbeuteten Zugangsdaten nutzt der Angreifer, um für Zahlungsempfänger des Unternehmens betrügerische Bankverbindungen zu hinterlegen.
- Management und Mitarbeitende sollten daher grundsätzlich darauf achten, in Sozialen Medien, auf der Webseite des Unternehmens oder gegenüber unbekannten Anrufern keine vertraulichen Informationen über interne Zuständigkeiten, Kundenbeziehungen und Geschäftsabläufen preiszugeben.



Private Mail-Accounts, Geräte und Netzwerke

- Besondere Risiken durch Cyber-Attacken bestehen, wenn geschäftliche Informationen digital an private E-Mail-Accounts, Geräte und Netzwerke übermittelt werden. Sie verlassen damit den technischen Schutz des Unternehmens.
- Management und Mitarbeitende sollten daher auf die Nutzung privater Anwendungen verzichten. Private Geräte sollten zu betrieblichen Zwecken nur dafür genutzt werden, um per VPN auf Netzwerke und Anwendungen des Unternehmens zuzugreifen.

Warnung vor Cyber-Angriffen im Zusammenhang mit Corona-Pandemie



Video-Konferenzen und Online-Kollaboration

- Cyber-Kriminelle könnten sich Zugang zu Telefon- und Video-Konferenzen verschaffen, wenn ihnen Anmeldedaten und Zeitpunkt einer Konferenz in die Hände fallen – etwa durch eine abgefangene oder irrtümlich weitergeleitete E-Mail. Organisatoren der Meetings sollten von Teilnehmern ein Passwort verlangen und ihnen dieses zuvor getrennt von der Meeting-ID übermitteln.
- Prüfen Sie, welche Video-Konferenz-Anwendungen Mitarbeitende konform der Bestimmungen des Datenschutzes nutzen können.
- Wegen der einfachen Bedienbarkeit nutzen derzeit bis zu 200 Millionen Menschen pro Tag die Video-Konferenz-App Zoom. Unbekannten kann es jedoch gelingen, sich Zugang zu einem Zoom-Call zu verschaffen, wenn der Organisator für diesen kein Passwort vergibt. Zudem bestanden oder bestehen technische Sicherheitslücken, die derzeit aber kein schwerwiegendes Risiko darstellen. Nutzer sollten die Zoom-App jedoch ständig aktualisieren und Calls mit Passwörtern schützen.
- Kollaborations-Anwendungen, wie zum Beispiel Google Docs oder Slag, erleichtern die Zusammenarbeit von räumlich getrennten Teams. Werden jedoch die Zugriffberechtigungen nicht gewissenhaft zugeteilt, kann auch Unbefugten der Zugriff auf die vertrauliche Kommunikation gelingen. Zum Beispiel, wenn sich Teilnehmer mit einer beliebigen privaten E-Mail-Adresse anmelden können.

Empfehlenswerte Sicherheitshinweise für Mitarbeitende im Home Office

- Verwenden Sie private E-Mail-Accounts, SMS und Social Media nicht für geschäftliche Zwecke.
- Nutzen Sie für sensible Telefonate über ein privates Smartphone die Anrufumleitung zur beruflichen Festnetznummer, sofern das möglich ist.
- Nutzen Sie für Video- und Telefonkonferenzen sowie als Kollaborations-Plattform nur die von Ihrem Unternehmen dafür freigegebene Lösungen.
- Speichern Sie sensible berufliche Informationen nur im geschützten Netzwerk Ihres Unternehmens und niemals auf privaten Speichermedien – weder auf der Festplatte Ihres Geräts, noch auf mobilen Speichermedien oder in Ihrer Cloud.

Warnung vor Cyber-Angriffen im Zusammenhang mit Corona-Pandemie

- Halten Sie Betriebssysteme und Software Ihres privaten Computers und auch des Heim-Routers durch regelmäßige Updates der Hersteller immer auf dem neusten Stand. Damit schützen Sie Ihre privaten sensible Daten und auch die Systeme Ihres Unternehmens, wenn Sie auf diese von Zuhause zugreifen.
- Installieren Sie auf privaten Geräten Virenschutzprogramme und halten Sie diese aktuell.
- Schützen Sie Ihren Router durch ein starkes und mindestens 24 Zeichen langes Passwort. Andernfalls könnten Kriminelle von fern Schadsoftware auf Ihren Geräten installieren. Aktuell leiten Cyber-Kriminelle auf diese Weise auf betrügerische Webseiten, die einen Bezug zur Corona-Pandemie haben.
- Sorgen Sie regelmäßig für Back-Ups Ihrer Daten.
- Verzichten Sie auf das automatische Ausfüllen von Eingabemasken in Ihrem Browser.
- Notieren Sie berufliche Kontakte nicht in Ihrem privaten Adressbuch Ihres Smartphones.
- Telefonieren Sie zu sensiblen beruflichen Anlässen niemals dort, wo andere mithören könnten.
- Sorgen Sie dafür, dass Ihnen niemand beim Arbeiten auf Bildschirm und sensible Dokumente schauen kann.
- Aktivieren Sie vor Pausen die Gerätesperre. Verwenden Sie ein sicheres Gerätepasswort, das nur Sie kennen.
- Achten Sie auch im Home Office auf Clear Desk.
- Nutzen Sie Social Media nur dann für Ihre berufliche Kommunikation, wenn Ihnen das ausdrücklich gestattet ist. Geben Sie in Ihren privaten Profilen keine beruflichen Informationen preis. Auch nicht, dass Sie womöglich gerade im Home Office arbeiten.