Kreissparkasse Böblingen

Phishing: Was muss ich wissen und erledigen?

Was ist Phishing?
Kriminelle verschicken betrügerische Nachrichten per E-Mail, über Messenger oder soziale Netzwerke. Ziel ist, dass Sie einen Anhang herunterladen (und somit ein Schadprogramm installieren) oder auf einen Link klicken. Auf der Seite werden Sie aufgefordert vertrauliche und persönliche Informationen wie Adress-, Kontakt- und Zugangsdaten, sowie Passwörter einzugeben. Die Phishingseiten sehen täuschend echt aus und verleiten dazu, die angefragten Daten einzugeben. Diese werden dann direkt zu den Betrügern übermittelt, welche die Daten kriminell nutzen.

Wie erkenne ich betrügerische Nachrichten?
- Die E-Mailadresse vom Absender ist meist leicht als „nicht glaubwürdig“ erkennbar
- Allgemeine Ansprache ohne Namen
- Schlechte Rechtschreibung und Grammatik
- Kein Logo der Kreissparkasse Böblingen, nur allgemeine Schriftzüge der „Sparkasse“
- Sie werden aufgefordert einen Link anzuklicken oder eine Datei/Anhang herunter zu laden

Betrügerische E-Mails können Sie im Original an warnung@sparkasse.de weiterleiten. Ihre Sparkasse verhindert damit die weitere Verbreitung.

Neben klassischen E-Mails nehmen auch betrügerische Telefonanrufe stark zu. Hierbei wird oft die Telefonnummer der Kreissparkasse Böblingen im Display eingeblendet. Lassen Sie sich davon nicht täuschen und legen Sie bei verdächtigen Anrufen einfach auf. Im Anschluss rufen Sie bitte direkt bei Ihrer Sparkasse an und versichern sich, dass der Anruf kein Betrug war.

Neu sind vor allem die immer häufiger versendeten Phishing-SMS. Als Absender der SMS finden Sie Namen wie „Sparkasse“ oder „Sparkassen-Kundenservice“. Auch hier gilt: Klicken Sie auf keine Links und fragen Sie ggf. bei Ihrer Sparkasse nach, ob die SMS von uns versendet wurde.

Ihr Enkel meldet sich über WhatsApp mit einer neuen Mobilfunknummer bei Ihnen und benötigt dringend Geld? Sie ahnen es schon – auch hier sind Kriminelle am Werk. Bleiben Sie ruhig, überweisen Sie kein Geld und wenden sich bei Fragen direkt an Ihre Sparkasse.

Das sollten Sie tun, wenn…

…Sie auf einen Link geklickt haben und **persönliche Daten angegeben** haben oder einen Anruf erhalten haben:
- Stellen Sie immer eine Strafanzeige bei der Polizei vor Ort.
- Achtung: Betrüger könnten Sie die nächsten Tage als Mitarbeiter Ihrer Sparkasse anrufen oder auf anderen Wegen kontaktieren. -> Seien Sie vorsichtig und verständigen Sie ggf. sofort die Polizei. Gehen Sie nicht auf die Aufforderungen ein!

…Sie auf einen Link geklickt haben und **Zugangsdaten angegeben** haben:
- Sperren Sie sofort Ihr Online-Banking (3x falsche PIN eingeben).
- Ändern Sie auf einem anderen, nicht infizierten Gerät sofort die Passwörter.
- Oft dient Ihre E-Mailadresse auch dazu, vergessene Passwörter wiederherzustellen, ändern Sie daher auch dieses Passwort.
- Ebenso Zugänge mit denen Sie sich auf anderen Plattformen anmelden können (z.B. Anmelden mit Facebook, …).

…Sie auf einen Link geklickt haben und **Zahlungsdaten angegeben** haben:
- Rufen Sie sofort den Sperrnotruf 116 116 an und sperren alle betroffenen Karten.
- Informieren Sie Ihre Sparkasse und kontrollieren Sie die Umsätze auf Ihren Konten.
- Ihre Sparkasse kann versuchen betrügerische Buchungen zurückzuholen.

…Sie einen **betrügerischen Anruf** erhalten haben:
- Beachten Sie alle oben genannten Punkte.
- Insbesondere bei z.B. betrügerischen Microsoftanrufen schalten sich die Cyber-Kriminellen auf Ihre Geräte mit auf. Trennen Sie in diesen Fällen schnellstmöglich die Internetverbindung auf den Geräten und schalten diese aus.
- Lassen Sie die Geräte von einem Spezialisten auf Schadprogramme überprüfen.

…Sie einen **Anhang/Datei heruntergeladen** haben:
- Trennen Sie die Geräte von der Internetverbindung.
- Lassen Sie die Geräte von einem Spezialisten auf Schadprogramme überprüfen.
- Ändern Sie alle Zugangsdaten von Plattformen bei denen Sie sich seit dem Download der Datei / dem Anhang angemeldet haben (z.B. E-Mailprogramme, Shopping-Accounts, …). Nutzen Sie hierzu ein anderes, nicht infiziertes Gerät.

So schützen Sie sich vor Phishing:
- Besuchen Sie www.kskbb.de/sicherheit um Informationen zu aktuellen Phishing-Mails und allgemeine Sicherheitsinformationen zu erhalten.
- Aktuelle Themen und Informationen von Ihrer Sparkasse erhalten Sie in unserem Newsletter. Sie können sich auf www.kskbb.de/newsletter anmelden.
- Benutzen Sie immer unterschiedliche Passwörter für alle Zugänge.
- Seien Sie skeptisch bei E-Mails mit Anhängen und Links (Klicken Sie nicht auf die Links und laden Sie keine Anhänge herunter)
- Installieren Sie auf allen Geräten, auch Smartphones, Antivirensoftware und halten Ihre Betriebssysteme und Software mit Updates auf dem aktuellen Stand.

Ihre
Kreissparkasse Böblingen

Dieses Informationsblatt gibt erste Informationen zum Thema „Phishing“ und erhebt keinen Anspruch auf Vollständigkeit. Bei einem Verdacht auf betrügerische Tatbestände wenden Sie sich bitte direkt an die nächste, örtliche Polizeistation.