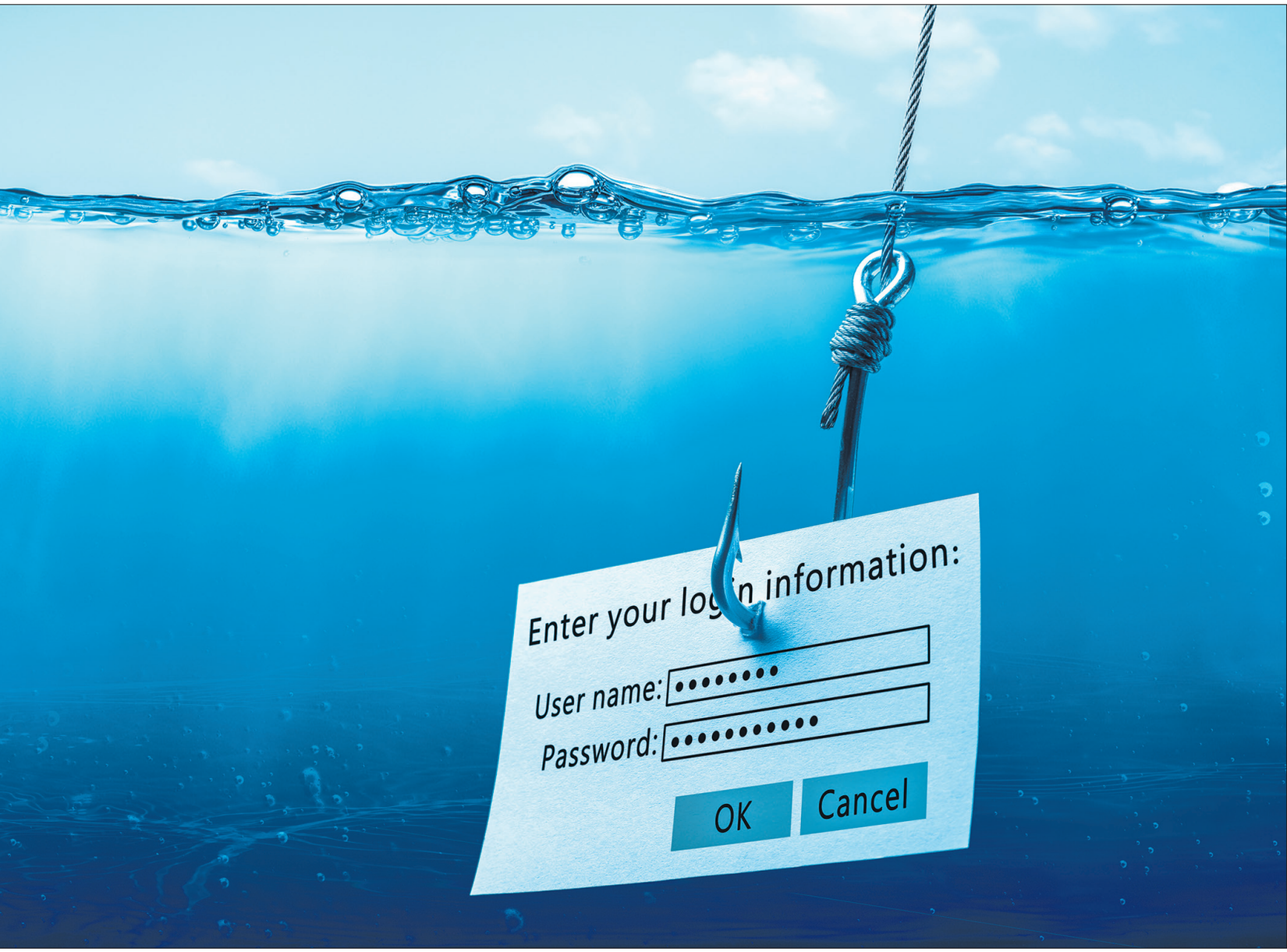


Ausgephisht

Die Sicherheitssysteme von Mac, Windows & Co. werden immer besser. Entsprechend weichen Internetverbrecher auf eine neue Schwachstelle aus: die Anwender. **Wir zeigen Ihnen, wie Sie betrügerische Nachrichten erkennen und damit umgehen.** ● VON LUCA DIGGELMANN

Einst waren Viren, Trojaner und ähnliche Schadprogramme der grösste Gefahrenherd am PC. Die digitalen Käfer gelangte meist über E-Mail-Anhänge und kompromittierte Downloads auf den PC und richteten dort direkt Schaden an. Entsprechend rüsteten sich Software-Hersteller wie Apple, Microsoft und Google gegen solche Angriffe und lernten genauer, diese zu verstehen und zu verhindern. E-Mails werden gescannt, Download-Links vom Webbrowser geprüft, Downloads vor Abschluss durch den Virenscanner gejagt. Das Resultat: Malware wird heutzutage vergleichsweise gut erkannt.

Direkte Angriffe mit Malware passieren zwar nach wie vor, sind aber weniger effizient geworden. Deshalb haben sich Onlinegauner angepasst und greifen vermehrt ein leichteres Ziel an: die User selbst, Bild 1. Und hier steht Phishing (siehe Box rechts) an oberster Stelle.

Phishing erkennen

Die Standard-Phishing-Nachricht ist einfach: Die Angreifer versuchen, Nutzer dazu zu bringen, auf einen Link zu klicken, Bild 2. Hinter diesem Link versteckt sich dann die nächste Stufe des Plans. Meistens handelt es sich um einen Malware-Download oder ein Formular, das heikle Daten abgreifen will. Im Folgenden erfahren Sie, wie Sie Phishing-Mails erkennen.

Bild: Shutterstock/Philip Steury Photography

Bild 1: Klassisches Phishing – mit schlechtem Deutsch und offensichtlich falschem Link

Bild 2: Diese SMS hat meine Frau erhalten. Wir haben keine Kinder. Fall abgeschlossen

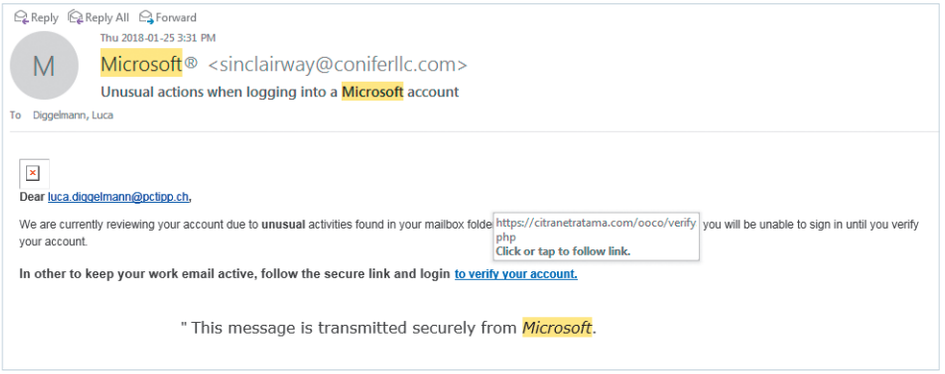


Bild 3: Geschäftsmail gesperrt? Genau mit solchen emotionalen Effekten arbeitet Phishing

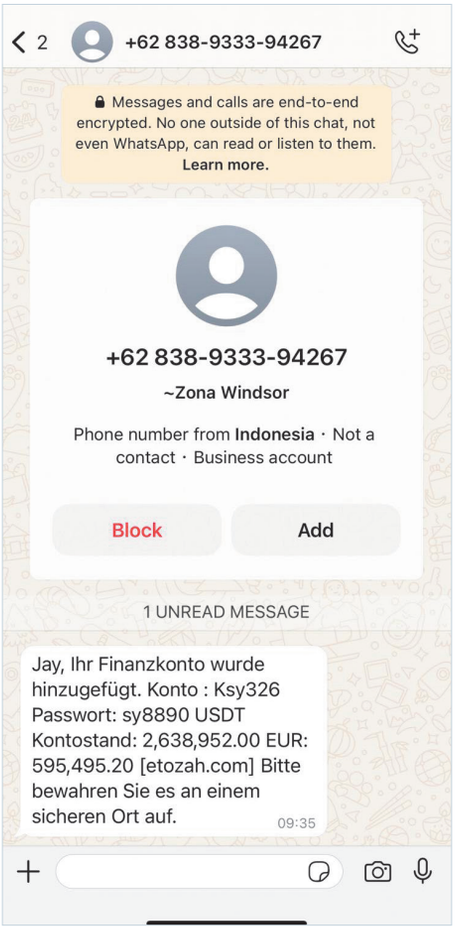


Bild 4: Plötzlich Millionär? Wohl kaum

Das Wichtigste vorweg: Immer wenn es um Geld geht, sollten Sie Ruhe bewahren, die Nachrichten genau anschauen und prüfen.

PLAUSIBILITÄT

Haben Sie ein UBS-Konto? Falls nein, ist die Log-in-Aufforderung für «Ihr» UBS-Konto wohl ein Fake. Sofern Sie nichts bestellt haben, wird auch die angekündigte UPS-Lieferung nicht echt sein – vor allem, wenn sie noch weitere der folgenden Punkte der Phishing-Erkennung beinhaltet.

HANDLUNG ERFORDERLICH

Phishing-Mails erwarten immer eine Handlung; fast immer explizit. Es soll ein Anhang geöffnet, ein Link geklickt, eine Datei heruntergeladen, ein Formular ausgefüllt, Geld überwiesen werden etc. Seltener sind Mails, auf die man Antworten soll, bei denen dann auch die Definition von Phishing etwas strapaziert wird.

In den meisten Fällen wird der Nutzer ausdrücklich dazu aufgefordert, eine Handlung zu unternehmen. Oftmals wird diese Handlung mit Druck unterlegt.

Seltener sind hingegen Nachrichten, bei denen die Aktion versteckt ist. Dabei handelt es sich meistens um Fälschungen von Bankmails oder ähnlichen Diensten. Beispielsweise erhält man einen verseuchten Bankauszug oder einen Link zum vermeintlichen Versicherungsportal. Da Banken und Versicherungen diese E-Mails meistens ohne aktive Aufforderung verschicken, tun es die Phisher ihnen genau gleich.

EMOTIONEN

Emotionale Manipulation ist ein Kernelement vieler Phishing-Versuche. Oftmals spielt Phishing mit der Angst, Bild 3. Es wird schockiert, gedroht und meistens auf die Zeit gedrängt. Das soll das rationale Denken der Nutzer aushebeln und sie zu emotionalen Reaktionen verleiten. Aber auch andere Gefühle werden eingespannt. Männer mit sexuellen Angeboten zu ködern, funktioniert seit Anbeginn der Menschheit und auch die menschliche Neugier kann leicht für Phishing instrumentalisiert werden, Bild 4.

EILE

Dieser Punkt fällt in die gleiche Kategorie wie die Emotionen, ist aber separat erwähnenswert. Phisher haben es meistens unglaublich eilig. Wenn Sie nicht SOFORT Ihr Konto reaktivieren, wird die «Migros Bank» NOCH HEUTE Ihr gesamtes Vermögen sperren. Und wenn Sie nicht SOFORT per Eingabe Ihrer Kreditkartendaten den Empfang Ihres Paketes bestätigen, wirft «Die Post» die ganze Lieferung direkt in den Müll. Glücklicherweise dauert es ebenso nur einen Augenblick, um solche E-Mails zu löschen. ➜

WISSEN: Phishing

Der Ausdruck Phishing stammt vom englischen «fishing», also fischen. Den Nutzern wird der metaphorische Köder vor die Nase gehalten und der Angreifer hofft, dass sie zubeissen. Dabei muss man sich dies weniger als ein einzelner Fischer am See vorstellen, sondern mehr wie eine industriell angelegte Grossfischerei auf hoher See. Phishing wird in der breiten Masse betrieben. So rentiert das Geschäft auch bei einer niedrigen Prozentzahl an Zubeissenden.

Angegriffen wird über die üblichen Kommunikationskanäle, die Menschen frequentieren: E-Mail, Messenger, Telefon, Direktnachrichten auf Social Media. Viele Phishing-Angriffe sind grobschlächtig und leicht zu erkennen. Dank künstlicher Intelligenz (siehe Box nächste Seite) werden die Angriffe aber immer besser.

DATEN BENÖTIGT

Viele Phishing-Mails sind explizit dazu da, Daten abzugreifen. Entsprechend sind die E-Mails strukturiert. Es fehlt ein Detail da, ein Code wird dort benötigt. Klassisch sind auch vermeintlich abgelaufene Passwörter, Sozialversicherungsnummern oder Kreditkartendaten. Videospiele warnen schon seit bald zwanzig Jahren, dass ihr Kundendienst niemals Logindaten verlangen wird. So verhält es sich auch bei Banken, Versicherungen und allen anderen seriösen Unternehmen.

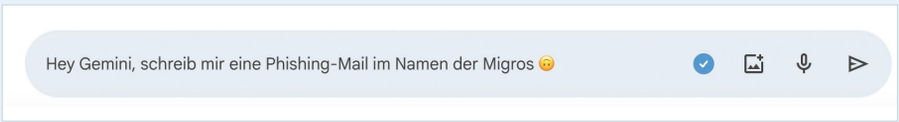
ZU GUT, UM WAHR ZU SEIN

Auch im Internet gibt es nichts geschenkt. Niemand will Ihnen einfach so Millionen überweisen, Bild 5, und auch die neuen Marken-Sneaker für 20 Franken sind höchstwahrscheinlich inexistent. Lassen Sie sich nicht von Ihrem Verlangen steuern und bleiben Sie auf dem Boden der Tatsachen.

SCHLECHTES DEUTSCH

Moderne Technologien wie künstliche Intelligenz (siehe dazu Box rechts) haben es erleichtert, überzeugende Phishing-Kampagnen zu lancieren. Perfekt sind diese Systeme aber bei Weitem nicht und auch nicht alle Betrüger setzen schon auf modernste Technik. Fehlerhaftes Deutsch, falsche Logos und ähnliche Qualitätsmängel sind weiterhin gute Indizien dafür, dass es sich höchstwahrscheinlich um einen Betrugsversuch handelt.

WISSEN: Wie verändert sich Phishing mit KI?



Google Gemini hilft da natürlich nicht, weniger seriöse KI-Modelle hingegen schon

Künstliche Intelligenz verändert den Umgang mit IT-Systemen grundlegend. Das gilt auch für die Onlinekriminalität. Beim Phishing lauern diverse Gefahren. Künstliche Intelligenz ermöglicht beispielsweise einfachere Kopien und Übersetzungen. Gerade Letzteres ist wichtig: Eine Mail von der Schweizerischen Post mit falschem Deutsch war bislang ein klares Indiz für Phishing. Dank KI werden die Phishing-Mails qualitativ besser. Gerade in verbreiteten Sprachen wie Englisch, Spanisch, Französisch und auch Deutsch wird die Qualität stark ansteigen und kaum noch als Indiz für Phishing zu gebrauchen sein.

Mit künstlicher Intelligenz wird auch das Social Engineering stärker werden. Mit nur wenig Ausgangsmaterial wird es immer einfacher, Bilder, Videos und sogar Stimmen zu manipulieren. Das eröffnet Kriminellen ungeahnte Möglichkeiten. Das gilt sowohl für die Qualität der Inhalte, als auch für die Automatisierung. Daten im grossen Stil sammeln und bündeln ist heute so einfach wie noch nie. In Zukunft werden vermehrt Verifikationsmethoden zum Einsatz kommen, da es rein inhaltlich schwierig wird, echt von gefälscht zu unterscheiden. Technische Lösungen wie digitale Signaturen, Passkeys oder Ähnliches helfen in dieser Hinsicht, bleiben aber weiterhin für menschliche Fehler anfällig. Und zuletzt bleibt wohl zur vollständigen Sicherheit nur noch der direkte Kontakt in der analogen Welt – zumindest bis zur Verbreitung täuschend echter Androiden.

LINKS & DOMAINS

Links sind ein Kernelement von Phishing. In den allermeisten Fällen werden Nutzer per Link auf eine falsche Webseite gelockt. Entsprechend sind Links ein guter Anhaltspunkt, um Betrug zu entlarven. Falsche Domains i und oberflächliche Verschleierung sind häufig. Zum Beispiel erhalten Sie eine E-Mail von «Die Post». Die E-Mail-Adresse lautet aber *info.post.ch@bschiss.tk*. Damit ist klar: Die Nachricht stammt von der Domain *bschiss.tk* und hat mit der Schweizer Post rein gar nichts zu tun.

Auch bei Links wird diese Technik verwendet, wobei hier die Domain wegen des fehlenden @ noch schwieriger zu finden ist. Üblich ist es auch, einen Linktext wie eine bestimmte Domain aussehen zu lassen, wobei der darunterlie-

Bild 7: Halten Sie Ihren Posteingang sauber

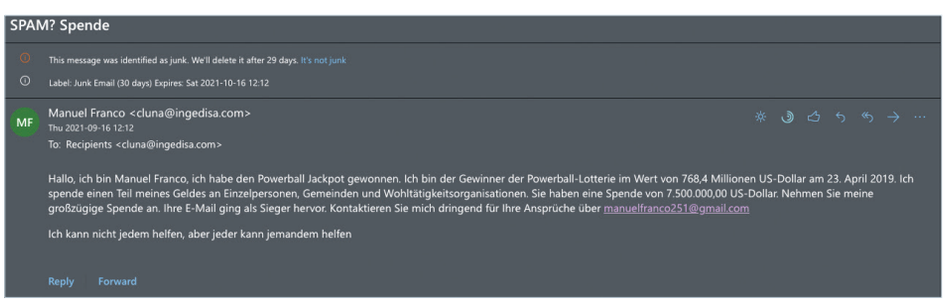


Bild 5: Also ich verscherble auch immer meine Lottogewinne an zufällige Mailadressen

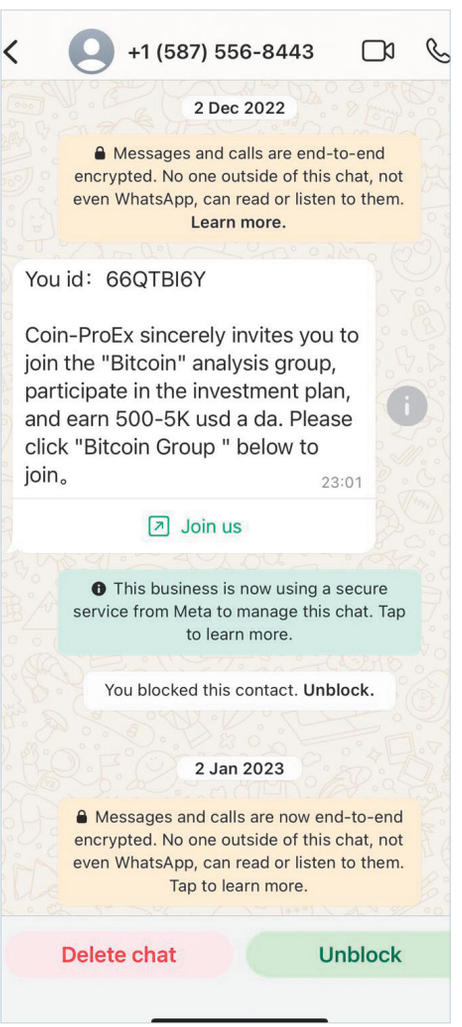


Bild 6: Auch auf Plattformen wie WhatsApp wird fleissig gephisht

Bild: Shutterstock/N Universe

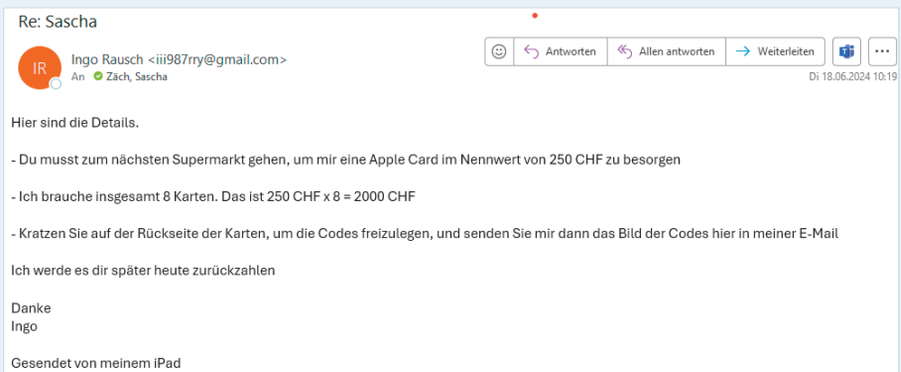
WISSEN: Social Engineering

Beim Social Engineering (soziale Manipulation) handelt es sich um eine Technik, die für gezieltere Angriffe gebraucht wird. Dabei gibt es verschiedene Angriffsmöglichkeiten. Beispielsweise kann ein Angreifer eine dem Opfer bekannten Person nachahmen, um an gewisse Daten zu kommen. Oder aber das Opfer wird selbst imitiert, um beispielsweise eine Bank oder einen Webdienst zu überlisten.

Oft bringen sich Angreifer per Social Engineering erst in eine gute Position, um danach mit Phishing und/oder Malware anzugreifen. Dazu ein Beispiel: Der Angreifer lädt sich einige öffentliche Fotos einer Person herunter und erstellt sich damit ein Instagram-Konto. Danach meldet sich der Angreifer vom neu erstellen Profil aus bei Bekannten des Opfers via Direktnachricht. Dabei erzählt er ihnen eine plausible Geschichte wie:

- das alte Konto sei gehackt worden.
- das sei ein neues Konto nur für enge Freunde.

Eventuell postet der Angreifer noch einige der gefundenen Fotos, um glaubwürdiger zu wirken. Anschliessend verbreitet der Angreifer Phishing-Links an die Freunde. Diese können unter Umständen auf dem falschen Fuss erwischt werden, da man von einem Freund ja nichts Böses erwartet und ihm gerne hilft.



Betrüger recherchieren über Ihr Umfeld und gehen danach gezielt auf Phishingtour

gende echte Link ganz anders heisst. Etwa: *post.ch/pakete* (*https://betrug.ch/formular*). Den echten Link sehen Sie nur, wenn Sie den Linktext in der Nachricht inspizieren (zum Beispiel mit der Maus darüber fahren, aber nicht drauf klicken) und genau hinsehen.

Und Achtung: Domains können gefälscht werden. Beispielsweise kann es durchaus sein, dass Sie eine E-Mail von einer Adresse mit *@post.ch* erhalten, die Nachricht aber gefälscht ist. Solches «Spoofing» wird derzeit technisch erschwert, ist aber noch immer verbreitet und erfordert einiges an Aufmerksamkeit.

Richtig handeln

Phishing greift via Routinen und Emotionen an. Entsprechend ist der beste Schutz dagegen die Kontrolle. Eine Schock-Nachricht versucht Sie zu emotionalem Reagieren zu verleiten. Statt zu reagieren, sollten Sie selbst agieren. Nehmen Sie die Fäden in die Hand und gehen Sie die Sache an wie ein Detektiv, der die Echtheit einer Nachricht prüfen will. Gute Techniken sind:

- **Innehalten:** Lassen Sie sich nicht stressen und denken Sie einen Moment nach, ob die Nachricht wirklich echt sein kann. Oftmals fallen Phishing-Mails schon durch die erste Welle rationalen Denkens durch, Bild 6.
- **Nachfragen:** Haben Sie eine Warnung Ihrer Bank erhalten? Rufen Sie bei Ihrer Filiale an (mit der Nummer aus dem letzten Auszug) und fragen Sie nach, ob die Nachricht echt sein kann. Gleiches gilt für verdächtige Nachrichten von Freunden oder Bekannten.
- **Selbst nachschauen:** Klicken Sie nicht auf den Link, um Ihr vermeintlich gesperrtes SBB-Konto zu reaktivieren. Tippen Sie stattdessen `sbb.ch` in Ihren Browser ein und loggen Sie sich wie gewohnt ein. Klappt alles wie üblich, war die E-Mail wohl falsch.
- **Recherche:** Kopieren Sie den Betreff oder Teile des Inhaltes der Nachricht und tragen Sie diese bei einer Suchmaschine ein. Oftmals finden Sie so schnell raus, ob eine Masche bereits bekannt ist. Das ist besonders praktisch bei Lockvogelangeboten.

All diesen Tipps ist etwas gemein: Sie übernehmen die Kontrolle. Das hebelt schon einen Grossteil der Erfolgsrezepte von Phishing aus.

Prävention

Wissen und ein gesundes Mass an Vorsicht sind die zwei besten Mittel gegen Phishing. Bilden Sie sich regelmässig weiter über neue Maschen und allgemein technologische Themen. Geben Sie wichtige Informationen nur dann heraus, wenn es nötig ist. Hier kann es auch helfen, wenn Sie mehrere E-Mail-Adressen verwenden. Davon ist eine für wichtige Dienste wie E-Banking, Behörden oder Versicherungen reserviert und eine weitere für weniger heikle Dinge. Weitere Sicherheitsebenen, beispielsweise für riskante Webseiten, können Sie nach eigenem Ermessen hinzufügen. Für Dienste, die Sie nur einmalig brauchen, lohnt sich der Einsatz von Wegwerf-Adressen, wie sie beispielsweise auf Apple-Geräten angeboten werden.

Ebenfalls hilfreich ist es, die eigene IT in Ordnung zu halten. Löschen und archivieren Sie E-Mails regelmässig und halten Sie Ihren Posteingang übersichtlich, Bild 7. So gehen Sie beruhigter an die Sache heran.

Zuletzt sollten Sie Phishing-Seiten und -Mails melden. Auf antiphishing.ch können Sie Links angeben. E-Mails leiten Sie an *reports@antiphishing.ch* weiter, Bild 8.

Bild 8: Hier können Sie Phishing-Mails und -Seiten einfach melden

Fachbegriff

Domain > Ein typisches Beispiel einer Domain ist www.pctipp.ch – eine Adresse, unter der ein PC im Internet erreichbar ist. Domains setzen sich meist aus drei Teilen zusammen. Zuvorderst steht die Subdomain (z. B. *www*). Im Anschluss folgt der Domainname (*pctipp*). Den Abschluss bildet die Top Level Domain wie *ch* oder *com*.