



Informationssicherheit: Im Comic packend verpackt



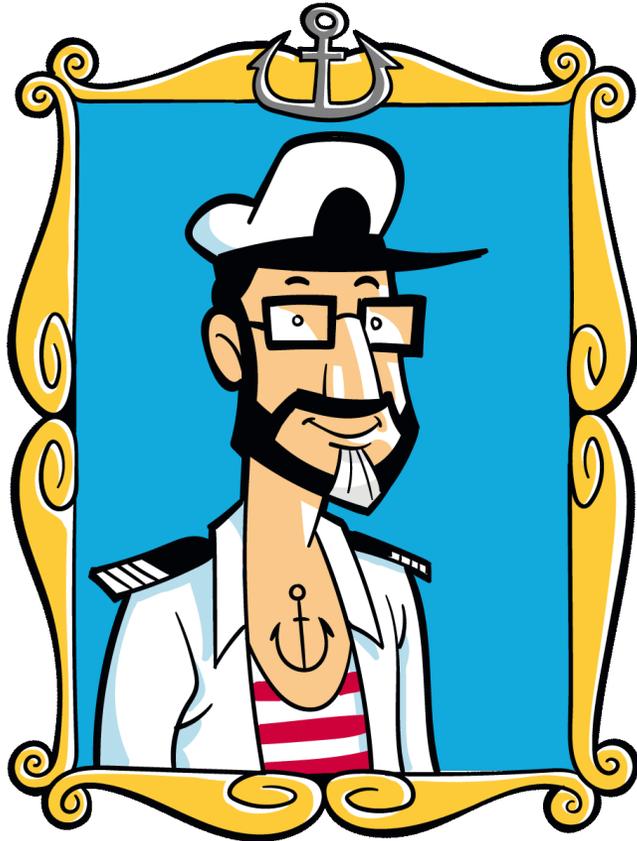
**Mit Käpt'n Safe & Easy mehr Aufmerksamkeit
für Ihre Cyber Security**



So lässt Informationssicherheit niemanden kalt



**Darf ich mich vorstellen:
Mein Name ist Käpt'n Safe**



Der wirksamste Schutz vor Cyber Crime sind neben entsprechender Technik vor allem Ihre Mitarbeiter. Wenn sie sensibilisiert sind für die Gefahren aus dem Netz und Cyber Security verinnerlicht haben. Doch herkömmliche Information und Aufklärung besitzt häufig nicht die notwendige Empathie, um Mitarbeiter wirklich zu erreichen und zu motivieren.

Dazu braucht es einen neuen, überraschenden, frischen und packenden Zugang. Den haben wir mit Hacker Island geschaffen. Sofort für Sie einsatzbereit und flexibel individualisierbar.

Und das ist mein Team



Easy



myEyeboard

Die folgenden Folien zeigen Ihnen, was wir für Sie mit „Hacker Island“ auf die Beine gestellt haben.



Aus dem Vollen schöpfen So vielfältig lässt sich Hacker Island einsetzen



Hacker Island ist ein komplettes Paket voller erprobter, ebenso informativer wie unterhaltsamer Materialien, die Sie auf vielfältige Weise einsetzen können – und das an vielen Stellen auf Ihr Unternehmen individualisierbar.

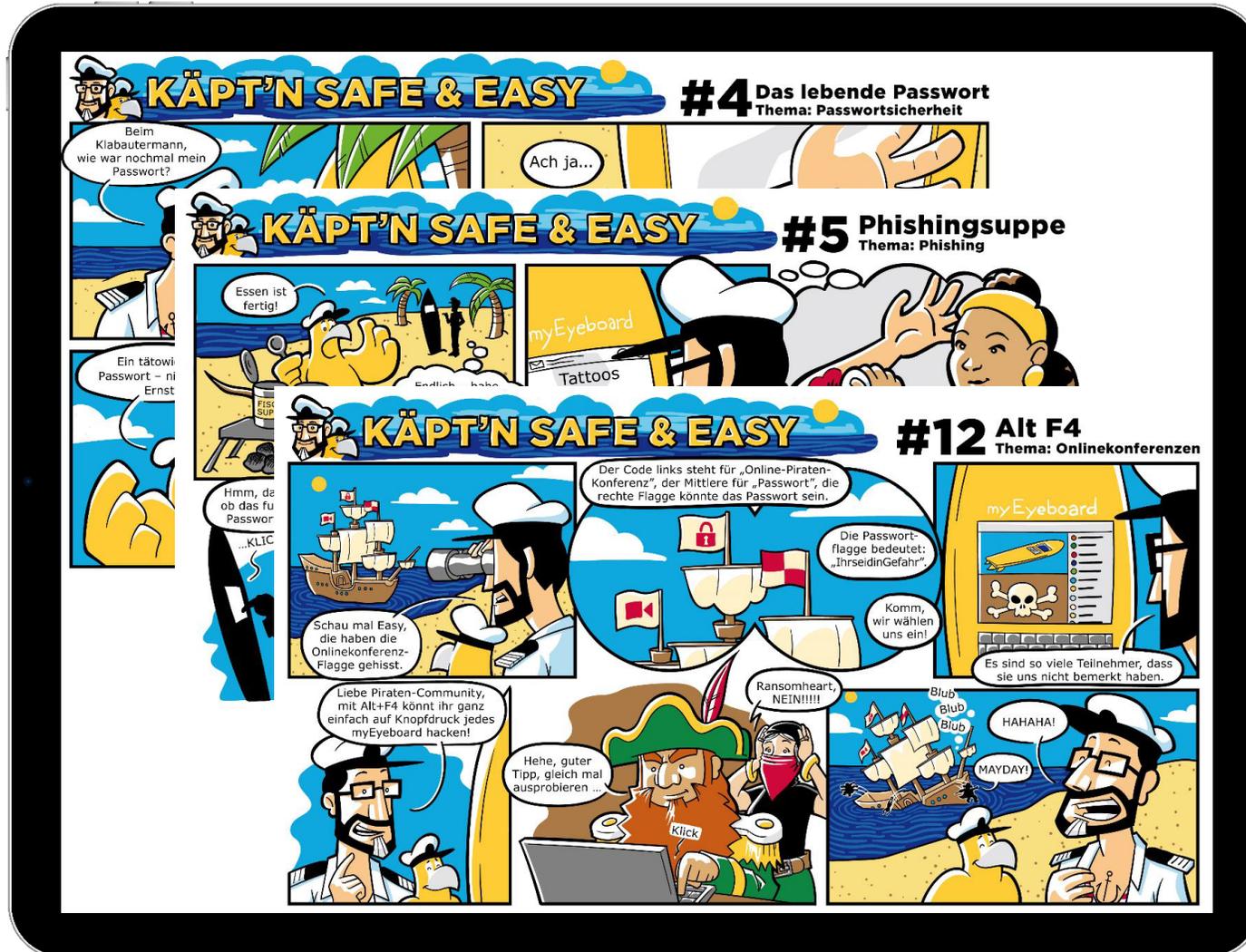
Die aufeinander abgestimmten Bausteine funktionieren als

- **umfassende Full-Service-Kampagne**, ohne dass Sie selbst etwas zu entwickeln brauchen, genauso wie
- **im Mix mit bei Ihnen bereits laufenden oder geplanten Maßnahmen**, also beispielsweise als ergänzende interne Website, Newsletter oder Schulungsprogramm.



Tolle Storys

36 thematisch ausgerichtete Comic-Strips



Die Themen der Comics decken auf ihre ganz eigene und überraschende Art die unterschiedlichsten Bereiche der Informationssicherheit ab, beispielsweise

- Wie gehe ich mit meinen Daten im Netz und in den sozialen Medien um?
- Was ist Social Engineering, Malware, Phishing, CEO Fraud etc.?
- Wie sichere, übertrage und entsorge ich Daten korrekt
- Welche besonderen Regeln gelten im Homeoffice?



Kompletter Background

36 Hintergrundartikel mit den wichtigsten Fakten



- Zu jedem Comic gibt es einen Hintergrundartikel mit detaillierten Erläuterungen. Diese Artikel können individuell auf die firmeninterne Situation angepasst werden.



Staffel 1 / Beispiel 1 - Artikel

Passwörter: Der Schlüssel zu unserem digitalen Leben

Passwörter sind wie sehr private Gegenstände unseres alltäglichen Lebens, die wir vermutlich niemals an andere verleihen und regelmäßig wechseln. Zum Beispiel Ihre Zahnbürste. Diese würden Sie auch nicht Ihren Kollegen leihen oder weitergeben, oder? Dies gilt selbstverständlich ebenfalls für Ihr Passwort. Denn wer Ihr Passwort kennt, handelt in Ihrem Namen, und Sie sind für diese Handlungen haftbar – ob Sie das wollen oder nicht! Wie bei Ihrer Wohnung, Ihrem Haus oder Auto sind Sie also persönlich für die Sicherung der Zugänge verantwortlich.

Starke Passwörter – keine Namen, Kürzel oder Zeichenfolgen!

Dabei ist es recht einfach, ein starkes Passwort zu bilden. Es sollte keine sinnvollen Bezeichnungen enthalten (also NICHT „trivial“ sein) und mindestens 8 Zeichen haben (je länger, desto besser) und aus Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen bestehen. Bitte wählen Sie für jeden Zugang ein eigenes Passwort. Wenn Ihr Passwort unberechtigten Dritten bekannt wird, ist wenigstens nur ein Zugang „gehackt“. Falls Sie diese Regeln noch nicht einhalten, sollten Sie sich Zeit nehmen, alle Ihre Passwörter zu ändern.

Ihr Passwort darf also niemandem außer Ihnen bekannt sein und für niemanden außer Ihnen zugänglich sein – also niemals aufschreiben! Übrigens: Für die private Anwendung existieren zahlreiche kostenfreie Programme, die als Passwortspeicher Ihre verschiedenen Passwörter unter einem Master-Passwort komfortabel verwalten (zum Beispiel KeePass).

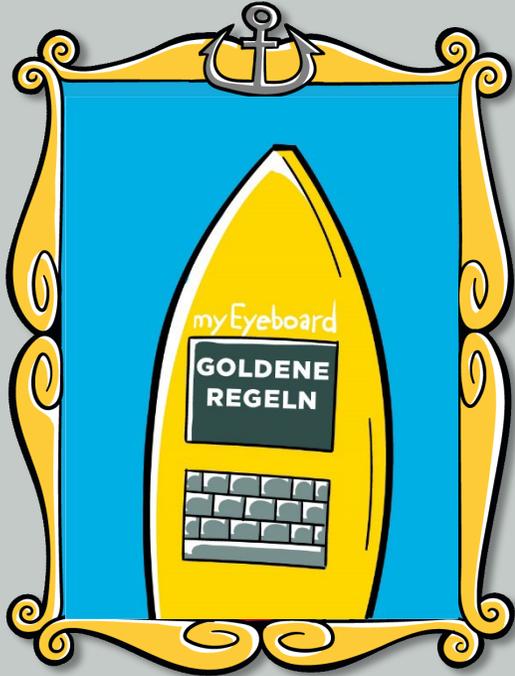
Ein neues Passwort – der Kreativität eine Chance geben.

Wahrscheinlich sind diese Informationen wie auch die Regeln zur Erzeugung „kryptischer“ Passwörter durch so genannte Memotechniken für die meisten von Ihnen keine Neuigkeiten. Dennoch zeigen sich wider besseren Wissens regelmäßig große Lücken bei der Authentifizierung. Warum? Bereits 2006 wurde in einer psychologischen Studie festgestellt, dass selbst sensibilisierte User gerne private Botschaften wie „EintrachtFrankfurt“ oder „Hansi“ in Passwörtern verwenden. Versuchen Sie, Ihren Gedanken einen Moment „Auslauf“ zu gönnen, wenn Sie ein neues Passwort vergeben. Vielleicht inspirieren Sie ja folgende Beispiele für die Bildung von Eselsbrücken:

Passwort	Bedeutung
WdAfmsamZa18h!	Während der Arbeit freue ich mich schon auf mein Zuhause ab 18 Uhr!
2009swidUguhv\$ä.	2009 sind wir in die USA geflogen und haben viele Dollars ausgegeben.

Konkrete to do's

36 Goldene-Regel-Textboxen



Phishing

- Öffnen Sie keine E-Mail-Anhänge und klicken Sie nicht auf Links in E-Mails von unbekanntem Absendern.
- Seien Sie achtsam bei Telefonanrufen vermeintlicher (Microsoft-)Supportmitarbeiter, installieren Sie keine Software nach Aufforderung von Dritten und lassen Sie keinen Fernzugriff zu. Sollten Sie eine Wartungsvereinbarung mit einem Dritten abgeschlossen haben, lassen Sie den Supportfall all

Ausspähen

- Denken Sie immer an potenzielle Zuschauer und Zuhörer: Auf der eigenen Terrasse, im Café oder während einer Zugreise lässt es sich mitunter angenehm, aber bestimmt nicht sicher arbeiten. Lassen Sie Ihren Laptop nicht unbeaufsichtigt.
- Gestalten Sie Ihren Arbeitsplatz so, dass eine Einsichtnahme von Dritten nicht möglich ist.
- Weitere potenzielle Zuhörer sind Alexa, Siri, Cortana – bitte deaktivieren Sie diese Assistenten in Ihrem Homeoffice-Bereich.
- Sperren Sie beim Verlassen des Arbeitsplatzes den Bildschirm. Bei Arbeitsende fahren Sie Ihren Rechner herunter.

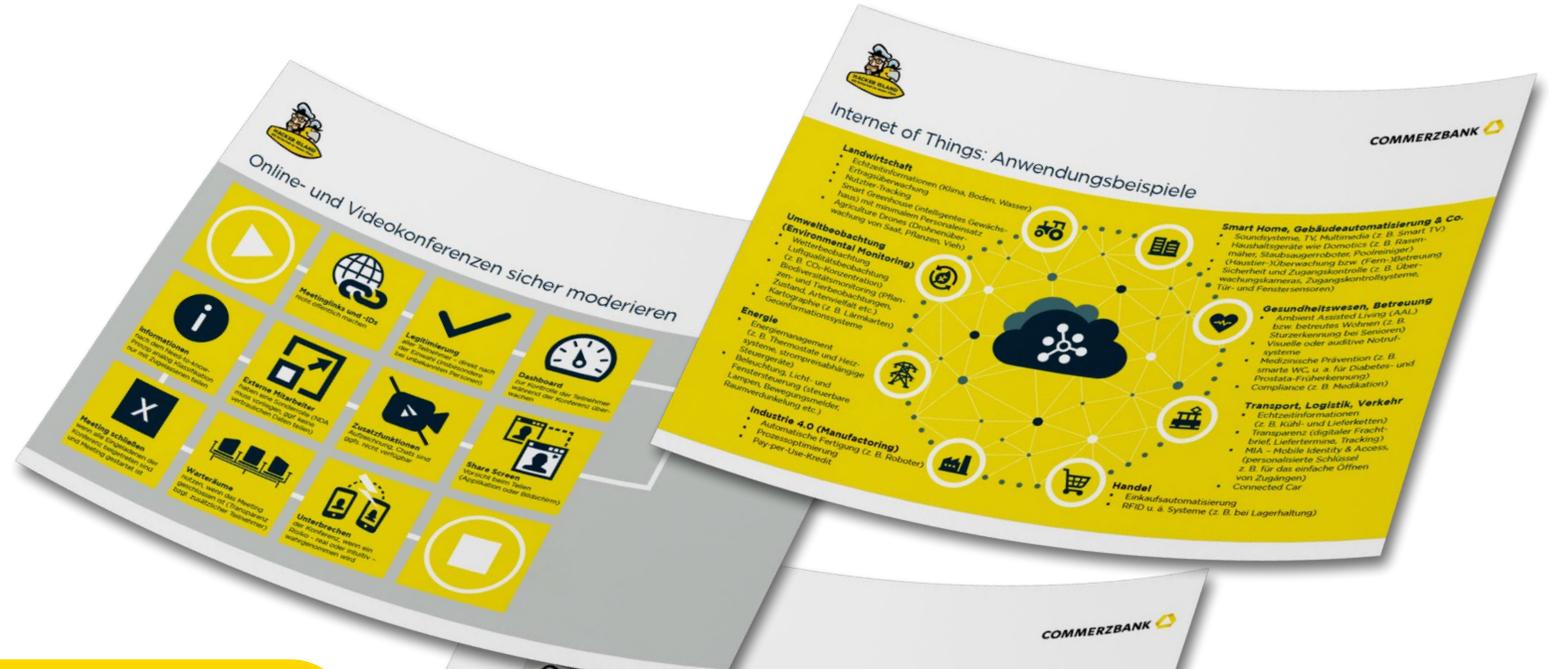
Am Ende jedes Artikels fassen „**Goldenen Regeln**“ das Thema zusammen und geben konkrete Handlungsempfehlungen..

Eingängige Aufbereitung zum Ausdruck fürs Büro: 16 Security-Infografiken, Illustrationen und Lernkarten

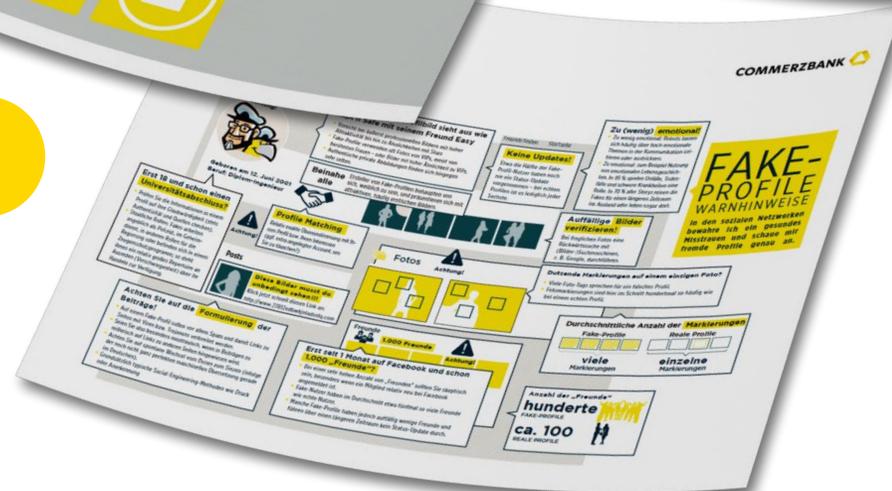


Ergänzend enthält Hacker Island Illustrationen, Übersichten und Lernkarten zum Ausdruck als

- ständiger Reminder im Büro
- Poster bei Präsenzs Schulungen
- Unterlage für den Schreibtisch



Hier ausdrucken



Was Sie bei der Umsetzung bitte beachten



Die Lizenz für Hacker Island enthält folgende Nutzungsbedingungen:

1. Die Lizenz gilt für das Unternehmen, das die Lizenz erworben hat – **nicht** für Tochterunternehmen oder weitere Unternehmen im Konzern.
2. Alle Unterlagen erhalten Sie **auf Deutsch und Englisch..**
3. Sie können Hacker Island **zeitlich unbegrenzt** nutzen.
4. Es gibt **keine Aktualisierungen**. Bitte prüfen Sie regelmäßig die Aktualität der Inhalte, um sie ggf. anzupassen.



Jetzt hier abschließen



**Ich bedanke mich für Ihre Aufmerksamkeit ...
... und wünsche viel Erfolg**



**Ihr Käpt'n
Safe & Easy**



KÄPT'N SAFE & EASY

Disclaimer



Wichtige Hinweise

Diese Information dient ausschließlich Informationszwecken und stellt weder eine individuelle Anlageempfehlung noch ein Angebot zum Kauf oder Verkauf von Wertpapieren oder sonstigen Finanzinstrumenten dar. Diese Ausarbeitung allein ersetzt nicht eine individuelle anleger- und anlagegerechte Beratung.

Die steuerliche Behandlung ist von den persönlichen Verhältnissen des Kunden abhängig und kann zukünftig Änderungen unterworfen sein. Die Commerzbank erbringt keine Beratung in rechtlicher, steuerlicher oder bilanzieller Hinsicht.

Diese Publikation darf ohne schriftliche Erlaubnis der Commerzbank AG weder vervielfältigt noch weiterverbreitet werden.

© Commerzbank AG 2023. Alle Rechte vorbehalten.





COMMERZBANK