informatiksicherheit.gr.ch
Eine Broschüre des Amtes für Informatik

IHR BEITRAG
ZUR INFORMATIONS-SICHERHEIT

Kanton Graubünden
Chantun Grischun
Cantone dei Grigioni

GEMEINSAM FÜR MEHR SICHERHEIT

Geschätzte Mitarbeiterin,
geschätzter Mitarbeiter

Die Informations- und Kommunikationstechnologie ist aus dem Alltag der kantonalen Verwaltung nicht mehr wegzudenken. In den Medien nehmen Berichte von gezielten Angriffen auf Informationen von Unternehmen oder Verwaltungen zu. Das Thema Datenschutz hat in vielen Dienststellen einen hohen Stellenwert.

Neben technischen Sicherheitsmassnahmen ist das verantwortungsbewusste Verhalten aller Mitarbeitenden die wichtigste Grundlage für die Sicherstellung der Informatik- und Informationssicherheit in der kantonalen Verwaltung. In bestimmten Bereichen können nur Sie verhindern, dass Schäden entstehen oder Persönlichkeitsrechte verletzt werden.

Diese Broschüre gibt Ihnen einen Überblick über die wichtigsten Regeln zum sicheren Umgang mit Informations- und Kommunikationstechnologie am Arbeitsplatz. Helfen Sie mit, wertvolle Daten zu schützen, welche im Auftrag der Bevölkerung bearbeitet werden.

Regierungsrätin Barbara Janom Steiner
Vorsteherin des Departements für Finanzen und Gemeinden

Eine Milliarde Android-Handys mit Sicherheitslücke

Hacker könnten über Lücken auf knapp eine Milliarde Android-Geräte zugreifen, warnt eine israelische Sicherheitsfirma. Mehr...

08.08.2016

500 Millionen Yahoo-Konten gehackt

Zwei Jahre lang hielt der Internet-Pionier den Datendiebstahl geheim. Nach der Übernahme durch den US-Telekomriesen Verizon gesteht Yahoo nun den **Hacker**-Angriff ein. Mehr...

22.09.2016

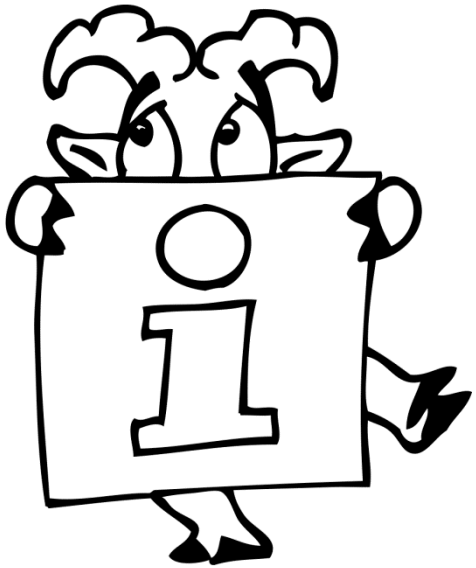
Hacker-Attacke gegen US-Demokraten grösser als gedacht

Erneut wurden die US-Demokraten gehackt, diesmal traf es das Wahlkampfkomitee der Partei im Repräsentantenhaus. Das FBI ermittelt. Julian Assange kündigt noch mehr Clinton-Material an. Mehr...

30.07.2016

Quelle: tagesanzeiger.ch

INFORMATIONSSICHERHEIT IN DER KANTONALEN VERWALTUNG



[1] In jeder Dienststelle gibt es neben dem Informatik-Verantwortlichen (IV) einen Informatik-Sicherheitsverantwortlichen (ISV). Der ISV ist Ihre Ansprechperson für alle Sicherheitsbelange.

[2] Auf der Intranetseite **http://informatiksicherheit.gr.ch** finden Sie alle Informationen und Weisungen zur Informatik-Sicherheit.

[3] Melden Sie Mängel, Sicherheitslücken, Viren-Vorkommen oder Sicherheitsvorfälle sofort dem ISV ihrer Dienststelle.

[4] Der Informatik-Sicherheitsbeauftragte (ISB) Tel. 3164, E-Mail isb@afi.gr.ch ist für die Informatik- und Informationssicherheit in der kantonalen Verwaltung zuständig.

[HINTERGRUND] Die Informatik-Verordnung (InfV) regelt den Einsatz der Informatik in der kantonalen Verwaltung. Die Weisungen über die Informatiksicherheit regeln das grundlegende Vorgehen im Bereich Informationssicherheit. Das Vorgehen orientiert sich am Standard des BSI (Bundesamt für Sicherheit in der Informationstechnik), und beinhaltet neben technischen auch administrative, personelle, organisatorische und physische Aspekte und Massnahmen.

"Sicherheit" besteht aus Aspekten der Datensicherheit, des Informationsschutzes und des Datenschutzes. Die Datensicherheit gewährleistet die Verfügbarkeit, Vertraulichkeit und Integrität der Daten. Der Informationsschutz bestimmt, ob Informationen öffentlich, intern, vertraulich oder geheim sind. Der Datenschutz regelt den Umgang mit Personendaten gemäss Datenschutzgesetz.

Sicherheits-Werkzeuge wie verschlüsselte USB Sticks oder ein IncaMail-Zugang (eingeschriebene E-Mails, die auch verschlüsselt sind) können via IV Ihrer Dienststelle beim Amt für Informatik beantragt werden.

Im Rahmen der zentralen, internen Weiterbildung kann ein Kurs zu den Themen Informationssicherheit und Datenschutz besucht werden. Weitere Informationen dazu finden Sie auf der Intranetseite des Personalamtes.

STARKE PASSWÖRTER

[1] Ein starkes Passwort ist folgendermassen aufgebaut:

- Besteht aus mindestens 8 Zeichen.
- Enthält Klein- und Gross-Buchstaben, Zahlen und Sonderzeichen.
- Enthält keine leicht zu erratenden Wörter oder Zahlen, wie z. B. Namen, Auto-Kennzeichen oder Begriffe aus einem Wörterbuch.
- Können Sie sich gut merken, andere aber nur schwer erraten, z. B. Son**nENsch00ein, fRan?zis57ka.

[2] Verwenden Sie nie dasselbe Passwort für verschiedene Anwendungen oder Internet-Dienstleistungen.

[HINTERGRUND] Passwörter müssen sicherstellen, dass nur Berechtigte Zugriff auf ein System oder bestimmte Anwendungen und deren Daten haben. Ansonsten besteht die Gefahr, dass Daten von Unberechtigten eingesehen, manipuliert oder gelöscht werden. Dies kann auch der Fall sein, wenn Sie dasselbe Passwort für mehrere Internet-Dienstleistungen verwenden, und einer der Anbieter kompromittiert wird.

Halten Sie Ihr Passwort auf alle Fälle geheim, und geben Sie es auch nicht an Mitarbeiter oder Vorgesetzte weiter. Ändern Sie das Passwort periodisch. Bei Verdacht auf Missbrauch ist das Passwort sofort zu ändern und der Verdacht der vorgesetzten Stelle zu melden. Der Datenschutzbeauftragte des Kantons Zürich bietet Online ein Passwort-Check an, mit dem Sie ein Passwort auf die Stärke prüfen können.

Ein Tipp, wie Sie sich gute Passwörter merken können: Bilden Sie einen Satz und merken Sie sich jeweils die ersten Buchstaben der einzelnen Wörter. Beispiel: Oiw14wnIg? = Ob ich wohl 2014 wieder nach Italien gehe?

Schützen Sie auch Ihre mobilen Geräte (Smartphones, Tablets), je nach Schutzbedarf, mit einem PIN oder einem starken Passwort.

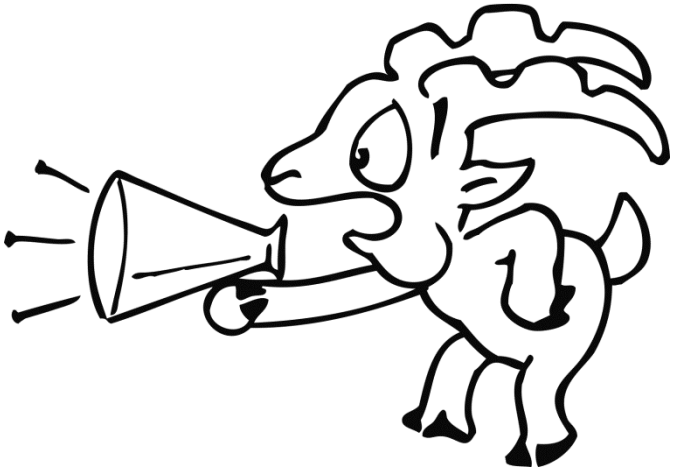
INFORMATIONSSICHERHEIT AM ARBEITSPLATZ

[1] Bei Abwesenheit während der Arbeitszeit:

- Computer sperren (z. B. Windows-Taste+L) sowie, abhängig von Abwesenheitsdauer und weiteren Sicherheitsmassnahmen (z. B. Gebäude- / Raum-Zutrittskontrollen) zusätzlich:
  - Keine vertraulichen Daten (Papiere, Dossiers, Datenträger) offen herumliegen lassen
  - Bürotür abschliessen, Fenster schliessen

[2] Am Feierabend und bei mehrtägigen Abwesenheiten zusätzlich:

- Dokumente und Datenträger mit vertraulichen Inhalten sowie mobile Geräte wegräumen und allenfalls einschliessen.
- Computer ausschalten



[HINTERGRUND] Physische Sicherheit (z. B. Schutz vor unberechtigtem Zutritt zu Ihrem Büro) ist, neben den technischen Massnahmen, ein wichtiger Sicherheits-Aspekt. Ein kurzer Augenblick genügt, um auf Ihrem Arbeitsplatz eine Schadsoftware zu installieren oder ein Gerät anzubringen, das Informationen nach aussen übermittelt.

Nehmen Sie keine Änderungen an Einstellungen des Betriebssystems oder Fachapplikationen vor, welche die Sicherheit beeinträchtigen. Damit Ihr Windows-Arbeitsplatz zuverlässig und sicher funktioniert, muss der PC regelmässig neu gestartet werden. Nur so werden Aktualisierungen vollständig abgeschlossen.

Setzen Sie am Arbeitsplatz keine privaten Geräte und keine privaten Programme ein.

Achten Sie auf unbekannte Personen, die sich im Gebäude aufhalten, und erkundigen Sie sich nach deren Absicht. Begleiten Sie Besucher während deren gesamtem Aufenthalt im Gebäude.

SICHERER UMGANG MIT E-MAIL

[1] E-Mails werden standardmässig nicht verschlüsselt und können von Dritten gelesen werden.

[2] E-Mail Absender können einfach gefälscht werden.

[3] Öffnen Sie Anhänge und folgen Sie Links in E-Mails nur, wenn Sie die Absender und den Inhalt als vertrauenswürdig einstufen.

[4] Eingehende E-Mails dürfen nicht automatisch an einen privaten E-Mail-Account weitergeleitet werden.

[5] Nutzen Sie die für Ihre Dienststelle verfügbaren technischen Möglichkeiten (z. B. IncaMail) für die sichere Übermittlung von vertraulichen Informationen an Adressaten ausserhalb der kantonalen Verwaltung.

[HINTERGRUND] Der Versand von E-Mails kommt dem Versand von Postkarten gleich. Ohne grossen Aufwand können die übermittelten Informationen gesammelt und ausgewertet werden. Geben Sie Ihre berufliche E-Mail-Adresse nur gezielt weiter. Setzen Sie Ihre E-Mail-Adresse nicht für private Zwecke ein. Vergewissern Sie sich, dass Sie E-Mails an die richtige Adresse senden.

Achtung vor Links in E-Mails: Immer häufiger werden E-Mails genutzt, um Sie auf Webseiten mit Schadsoftware zu locken (Phishing). Kontrollieren Sie deshalb Links in E-Mails auf Ihre Richtigkeit (mit der Maus über den Link fahren und die angezeigte Adresse vergleichen, noch nicht klicken). Geben Sie niemals Passwörter per E-Mail bekannt.

Das Amt für Informatik prüft eingehende E-Mails auf Spam und Viren. Virenverseuchte E-Mails werden direkt gelöscht, der Umgang mit Spam ist im Dokument Anleitung zur Filterung von Spam-Mails beschrieben.

Die automatische Weiterleitung an einen privaten E-Mail-Account ist nicht gestattet. Bei Abwesenheit ist der Auto-Responder einzurichten. Sofern E-Mails an mehrere Empfänger versandt werden, sind nach Möglichkeit Verteilerlisten oder die „Bcc-Option“ zu nutzen, so dass der Empfänger nicht die komplette Empfängerliste einsehen kann.

Private Nutzung von Internet und E-Mail: Die vorgeschriebene Arbeitszeit ist für die Erfüllung der dienstlichen Aufgaben zu verwenden (Personalverordnung PV Art. 58). Dienstliche Einrichtungen dürfen für private Angelegenheiten nur in notwendigen Fällen benützt werden (PV Art. 59). Für die private Nutzung ausserhalb der Arbeitszeit kann ein Antrag beim AFI ausgefüllt werden.

SICHER SURFEN IM INTERNET

[1] Verändern Sie die Sicherheitseinstellungen Ihres Internet-Browsers am Arbeitsplatz nicht.

[2] Laden Sie keine Dateien oder Programme aus dem Internet herunter, deren Ursprung sie nicht kennen oder als nicht vertrauenswürdig einstufen.

[3] Programminstallationen dürfen nur durch die dafür verantwortlichen Mitarbeiter (in der Regel der Informatik-Verantwortliche) freigegeben werden.

[4] Schon der Besuch einer verseuchten Webseite kann Ihren Arbeitsplatz infizieren, besuchen Sie keine Webseiten denen Sie nicht vertrauen.

[5] Beachten Sie Warnungen des Browsers, und besuchen Sie keine Seiten, bei welcher der Browser vor einem ungültigen Zertifikat warnt.

[6] Lesen Sie Meldungen, Nachrichten und Aufforderungen auf Internetseiten genau und vertrauen Sie ihnen nicht blind.

[HINTERGRUND] Programme, die Sie aus dem Internet herunterladen, können auf Ihrem Arbeitsplatz Schaden anrichten oder Ihre Tätigkeiten ausspionieren. Wenden Sie sich an den Informatik-Verantwortlichen Ihrer Dienststelle, wenn Sie ein zusätzliches Programm brauchen.

Seien Sie vorsichtig mit vertraulichen Informationen oder Personendaten.

Geben Sie bei der Nutzung von Internetdiensten wie z. B. Doodle keine vertraulichen Informationen preis. Aus Gründen der Sicherheit ist der Zugriff auf bestimmte Webseiten gesperrt.

Wenn ein Browser eine verschlüsselte Verbindung mit der aufgerufenen Internetseite aufgebaut hat, ist dies daran zu erkennen, dass am Beginn der Webseiten-Adresse dem "http" ein "s" angehängt wurde. Falls vertrauliche Daten bearbeitet werden, sollte die Website über eine solche https-Adresse aufgerufen werden. Bei jedem Aufruf einer https-Adresse prüft der Browser, ob der Anbieter der Internetseite ein gültiges Zertifikat vorweisen kann. Kann er das nicht, warnt der Browser mit einer Nachricht. Bei einer solchen oder ähnlichen Warnung des Browsers sollten Sie nicht auf der jeweiligen Webseite weitersurfen.

Private Nutzung von Internet und E-Mail: Die vorgeschriebene Arbeitszeit ist für die Erfüllung der dienstlichen Aufgaben zu verwenden (Personalverordnung PV Art. 58). Dienstliche Einrichtungen dürfen für private Angelegenheiten nur in notwendigen Fällen benützt werden. (PV Art. 59). Für die private Nutzung ausserhalb der Arbeitszeit kann ein Antrag beim AFI ausgefüllt werden.

DATENSCHUTZ

[1] Der Datenschutz dient dem Schutz der Persönlichkeitsrechte und der Privatsphäre.

[2] Öffentliche Organe dürfen Personendaten nur aufgrund einer rechtlichen Grundlage, nur für den angegebenen Zweck und nur soweit erforderlich bearbeiten.

[3] Vor der Eröffnung von neuen Datensammlungen ist eine datenschutzrechtliche Beurteilung vorzunehmen.

[4] Informieren Sie sich über den Datenschutz, falls Sie in Ihrer Dienststelle Personendaten bearbeiten.

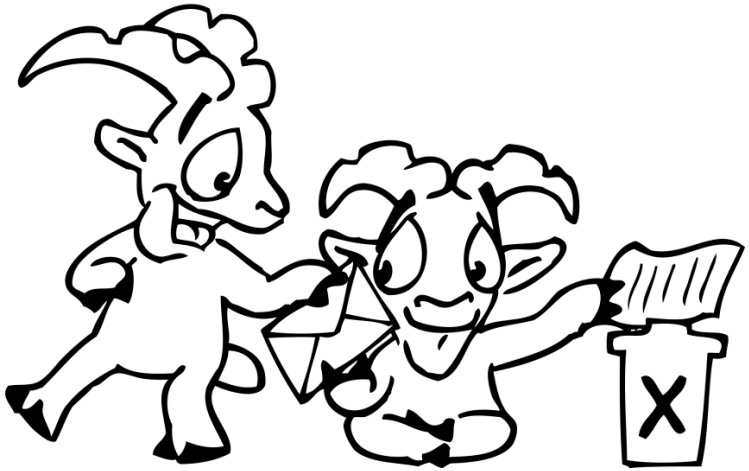
[5] Besonders schützenswerte Personendaten (gemäss Datenschutzgesetz) dürfen nur innerhalb der Schweiz gespeichert werden. Dies ist besonders bei Cloud-Dienstleistern zu beachten.

[HINTERGRUND] Der Datenschutz betrifft Personendaten. Das sind Informationen, die etwas über eine Person aussagen: Personalien, Angaben über Einkommen und Vermögen, Angaben über das Arbeitsverhältnis usw. Besonders schützenswerte Personendaten sind sensible Daten, die wegen einer erhöhten Gefahr für die Persönlichkeitsrechte stärker geschützt sind.

Dazu gehören: Die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre, die Rassenzugehörigkeit oder die ethnische Herkunft, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen oder Sanktionen. Der Datenschutz verpflichtet die Datenbearbeiter zu rechtmässigem und verhältnismässigem Handeln und verleiht den betroffenen Personen durchsetzbare Rechte. Datenbearbeiter müssen sich an Rahmenbedingungen halten. Öffentliche Organe dürfen Daten nur aufgrund einer rechtlichen Grundlage, nur für den angegebenen Zweck und nur soweit erforderlich bearbeiten. Die betroffenen Personen können gegenüber den öffentlichen Organen Rechte geltend machen. Sie haben Anspruch auf Auskunft, welche Daten über Sie bearbeitet werden. Unter gewissen Voraussetzungen können Sie die Berichtigung, Sperrung oder Löschung der Daten verlangen.

Die rechtlichen Grundlagen bilden das Bundesgesetz über den Datenschutz, sowie das kantonale Datenschutzgesetz. Falls Sie Fragen zum Datenschutz haben, melden Sie sich beim kantonalen Datenschutzbeauftragten.

SPEICHERN UND LÖSCHEN VON **DATEN**



[1] Speichern Sie Daten nur auf offiziellen Laufwerken und Fachapplikationen Ihrer Dienststelle.

[2] Löschen Sie Daten unwiederbringlich, bevor Sie ein Gerät oder einen Datenträger weitergeben. Mit einem einfachen «löschen» vernichten Sie Daten nicht definitiv. Die zuständigen Informatikmitarbeiter (in der Regel der Informatik-Sicherheitsverantwortliche) können Sie unterstützen.

[3] Stellen Sie beim Drucken von klassifizierten Informationen auf gemeinsam genutzten Geräten sicher, dass Dritte keinen Zugang zu den gedruckten Dokumenten haben.

[4] Schützenswerte Informationen auf Papier müssen im Aktenvernichter zerstört werden.

[HINTERGRUND] Daten, die Sie auf Server-Laufwerken des IKT-Leistungserbringers, Geschäftsverwaltungssystemen oder Fachanwendungen speichern, werden regelmässig gesichert. Für die Sicherung von Daten auf lokalen oder externen Datenträgern sind Sie jedoch selbst verantwortlich.

Je nach Drucker-Infrastruktur steht beim Drucken von vertraulichen Informationen auf gemeinsam genutzten Geräten die Funktion «Vertrauliches Drucken» zur Verfügung. Diese kann über den Druckertreiber eingestellt werden. Dadurch wird das Dokument erst nach Eingabe des Passworts am Drucker ausgegeben. Niemand anders kann Ihr Dokument lesen.

Das Amt für Informatik bietet eine einfache Lösung für das Verschlüsseln von Daten auf einem USB-Stick sowie eine verschlüsselte und vertrauenswürdige Übermittlung von E-Mails (IncaMail). Erkundigen Sie sich dazu bei ihrem Informatik-Verantwortlichen.

Elektronische Daten bleiben auch nach dem Löschen mit der Delete-Taste oder der Funktion «löschen» lesbar, es werden nur die Informationen zum Speicherort entfernt. Für die endgültige Vernichtung muss der Speicherort der Information mehrfach überschrieben werden. Für diesen Vorgang, auch "Wipen" genannt, stehen spezielle Programme zur Verfügung.

Entsorgen Sie Festplatten und externe Datenträger sicher, dazu gehören auch Tablets und Smartphones. Erkundigen Sie sich dazu bei ihrem Informatik-Verantwortlichen.

MOBIL UNTERWEGS

[1] Jeder Laptop, der ausserhalb der Büroräumlichkeiten eingesetzt wird, muss mit einem Festplatten-Verschlüsselungsprogramm ausgestattet sein, sofern der Schutzbedarf dies erfordert.

[2] Alle Laptops müssen für die Aktualisierung des Virenschutzes und für Sicherheitsupdates regelmässig ans kantonale Netz angeschlossen werden.

[3] Wer unterwegs mit mobilen Geräten arbeitet, muss beachten, dass Unbeteiligte auf den Bildschirm des Laptops oder Tablets sehen und die Gespräche auf dem Mobiltelefon mithören können.

[4] Der Verlust mobiler Geräte muss sofort dem ISV Ihrer Dienststelle gemeldet werden.

[HINTERGRUND] Laptops, Smartphones und Tablets müssen besonders geschützt werden, da sie nicht nur im eigenen Büro, sondern auch in der Öffentlichkeit verwendet werden.

Vermeiden Sie die Nutzung von unpersönlichen Geräten für den Zugriff auf oder die Bearbeitung von geschäftlichen Informationen (z. B. PC in Hotelhalle oder im Internetcafé).

Bearbeiten Sie interne, vertrauliche Daten oder besonders schützenswerte Personendaten nur auf offiziellen, von der kantonalen Verwaltung zur Verfügung gestellten mobilen Geräten. Ausgenommen davon sind vom AFI zentral verwaltete private Smartphones.

Sicherheitseinstellungen von Smartphones und Tablets, welche auf Daten im Intranet zugreifen können, werden vom Amt für Informatik zentral verwaltet. Bei Verlust oder Diebstahl können die Daten gelöscht werden. Verändern Sie keine Sicherheitseinstellungen, und installieren Sie nur vertrauenswürdige Apps.

Verbinden Sie sich nur mit vertrauenswürdigen Drahtlos-Netzwerken (WLAN).

Melden Sie den Verlust oder auch auffälliges Verhalten (z. B. häufiger Datenverkehr im Hintergrund) Ihres mobilen Gerätes umgehend dem ISV Ihrer Dienststelle.

SOCIAL ENGINEERING

[1] Social Engineering ist eine Methode, um durch Täuschung unberechtigten Zugang zu Informationen zu erlangen.

[2] Zur Ausbreitung von Schadsoftware werden oft Methoden des Social Engineering angewandt, etwa wenn der Name des E-Mail-Anhangs mit einem Virus einen besonders interessanten Inhalt verspricht oder der Absender angeblich aus der kantonalen Verwaltung stammt.

[3] Der Informatik-Dienstleister fordert Sie nie auf, vertrauliche Informationen wie ein Passwort per E-Mail oder am Telefon bekannt zu geben.

[4] Lassen Sie sich nicht ausfragen, einschüchtern oder bedrohen, und geben Sie keine vertraulichen oder sicherheitsrelevanten Informationen an Unbekannte weiter.

[HINTERGRUND] Wo Angreifer dank technischer Sicherheitsmassnahmen nicht weiterkommen, versuchen sie Anwender auf andere Weise zur Installation von Schadsoftware oder Herausgabe sensibler Daten zu bewegen.

Vergleichbar mit dem Trickbetrug an der Haustür setzen auch Angreifer im Internet auf die Vortäuschung einer persönlichen Beziehung zum Opfer oder machen Gewinnversprechen.

Viele weitere Varianten dieser Social Engineering genannten Vorgehensweisen sind denkbar und werden eingesetzt. Zum Teil wird dabei auch ein indirekter Kontakt über Freunde des eigentlichen Opfers gewählt.

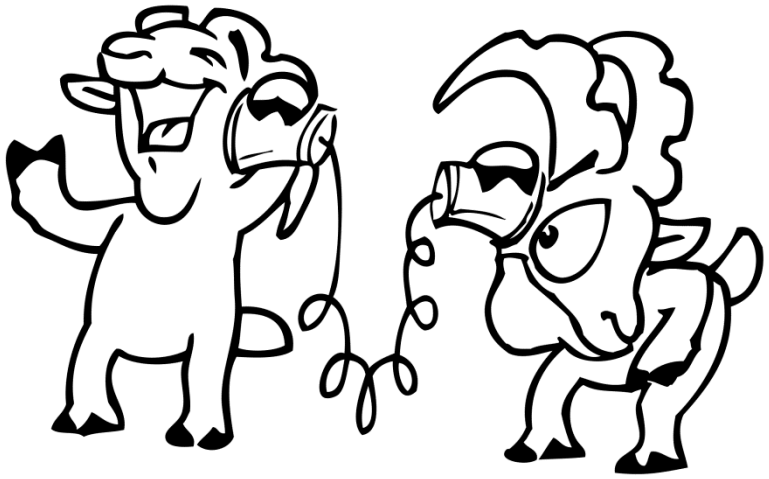
Phishing ist eine spezielle Form eines Social-Engineering-Angriffs. Mit Hilfe gefälschter Webseiten versuchen Betrüger an vertrauliche Daten wie z. B. die Kreditkartennummer oder Passwörter zu gelangen. Vertrauen Sie Meldungen, Nachrichten und Aufforderungen nicht blind. Klicken Sie nicht auf beliebige Angebote, auch wenn diese noch so verlockend klingen.

Haben Sie Zweifel an der Integrität einer Webseite, suchen Sie im Impressum nach einer Telefonnummer und verschaffen Sie sich telefonisch einen Eindruck von der Situation.

Bei merkwürdigen Nachrichten von Freunden rufen Sie diese an und fragen Sie nach, ob die Nachricht wirklich von dem oder der Bekannten stammt.

Vorsicht bei gefundenen USB-Sticks, setzen Sie gefundene USB-Sticks oder solche unbekannten Ursprungs nie ein. Seien Sie wachsam und vorsichtig.

UMGANG MIT **SOCIAL MEDIA**



[1] Aussagen im Namen des Arbeitgebers sind nicht zulässig.

[2] Für die private Nutzung darf in keinem Fall die geschäftliche E-Mail-Adresse oder das Kantonslogo verwendet werden.

[3] Veröffentlichen Sie in sozialen Netzwerken so wenig Informationen über Ihre berufliche Tätigkeit wie möglich.

[4] Bedenken Sie: Social Media sind noch öffentlicher als ein Bus oder ein Stammtisch. Für publizierte Inhalte sind Sie verantwortlich und Sie können dafür auch rechtlich belangt werden.

[HINTERGRUND] Social Media bezeichnen elektronische Medien, die es Nutzerinnen und Nutzern ermöglichen, miteinander zu kommunizieren und mediale Inhalte zu tauschen oder gemeinsam zu gestalten. Zu den Social Media gehören sowohl Netzwerke wie Facebook, Twitter, LinkedIn und XING als auch Websites wie Youtube und Wikipedia. Auch Blogs, Chats und Foren sind Teil der Social Media.

Pflegen Sie auf Social Media einen respektvollen und höflichen Umgang. Ironie, harsche Reaktionen oder Humor auf Kosten des Dialogpartners oder Dritter sind tabu. Verstecken Sie sich nicht hinter anonymen Spitznamen, sondern weisen Sie sich mit Ihrem Namen aus. Das geistige Eigentum und das Recht am eigenen Bild sind gesetzlich geschützt. Dokumente sowie fremde Bilder, Texte, Video, etc. ohne Nutzungsrecht gehören nicht ins Internet. Publizieren Sie nur Bilder und Texte, die sie auch jederzeit Ihren Kolleginnen und Kollegen, Mitarbeitenden oder Vorgesetzten zeigen würden. Denken Sie daran: Das Internet vergisst nichts. Einmal im Internet veröffentlichte Daten können zwar auf der betreffenden Seite entfernt werden, sie sind aber bereits unkontrolliert verbreitet und gespeichert worden.

Mit der privaten Nutzung von Social Media verhält es sich gleich wie mit der privaten Nutzung des Internets: Beschränken Sie Ihre privaten Aktivitäten am Arbeitsplatz auf ein Minimum. Wenn Sie über Social Media zu Fragen kontaktiert werden, die Ihren Arbeitgeber betreffen, verweisen Sie an den Mediendienst der Standeskanzlei (Tel. 2247, E-Mail: luzi.buerkli@staka.gr.ch).

INFORMATIK-SICHERHEIT **PRIVAT**

[1] Daten- und System-Backup einrichten.

[2] Anti-Virus-Software installieren.

[3] Software regelmässig aktualisieren (besonders Betriebssystem, Browser, Java, PDF-Reader).

[4] Personal Firewall aktivieren (Windows Firewall bietet "nur" Grundschutz).

[5] Starke Passwörter wählen und diese nur einmalig verwenden.

[6] Vertrauliche Daten auf externen Datenträgern oder Cloud-Storage-Diensten verschlüsseln.

[HINTERGRUND] Ihr Arbeitsplatz in der kantonalen Verwaltung bietet einen Grundschutz, welcher zu Hause nicht automatisch vorhanden ist.

Bearbeiten Sie keine schützenswerten Daten der kantonalen Verwaltung auf privaten Geräten.

Schützen Sie sich, indem Sie oben genannte Punkte beachten. Die folgenden frei erhältlichen Programme helfen ihnen privat:

- Anti-Virus-Software z. B. "Microsoft Security Essentials" oder "AntiVir"
- Daten verschlüsseln mit z. B. "TrueCrypt"
- Passwort-Safe verwenden, z. B. "KeePass"
- Vor Weitergabe von Geräten oder Datenträgern Daten sicher löschen, z. B. mit "Eraser"

Weitere Informationen, auch zu aktuellen Themen und Sicherheitslücken, finden Sie unter https://www.bsi-fuer-buerger.de

Version
Dezember 2016

Herausgeber
Informatik-Sicherheitsbeauftragter,
Amt für Informatik

Konzept Layout
Grafikdeal

Illustrationen
Rolf Giger

Die Broschüre kann vom Intranet des Amtes für Informatik oder unter http://informatiksicherheit.gr.ch heruntergeladen und gedruckt werden.