E-Mails und Anhänge

Viren und sonstige schädliche Software werden am häufigsten verbreitet über
— E-Mails (verseuchte Anhänge)
— USB-Sticks
— Internet-Webseiten

Phishing ist eine Methode von Betrügern, um sich Informationen von ihren Opfern zu beschaffen, die zur persönlichen Bereicherung eingesetzt werden können. Phishing-Angriffe erfolgen oft via E-Mails, in denen die Empfänger mit möglichst glaubhaften Geschichten dazu gebracht werden sollen, dem Absender vertrauliche Informationen preiszugeben.

Das Wichtigste in Kürze

- ☐ Misstrauen Sie E-Mails, deren Absender Sie nicht kennen oder deren Inhalt Ihnen verdächtig vorkommt.
- ☐ Fahren Sie mit dem Mauszeiger über die Internet-Adresse in der E-Mail, ohne zu klicken: So sehen Sie, auf welche Website der Link führt.
- ☐ Öffnen Sie bei verdächtigen E-Mails nie ein angehängtes Dokument oder Programm und klicken Sie auf keine darin angegebenen Links.
- ☐ Öffnen Sie keine Anhänge, die zwei Endungen aufweisen (z. B. foto.jpg.vbs).
- ☐ Seriöse Unternehmen fragen nie per E-Mail nach persönlichen Daten.
- ☐ Kommen Sie E-Mail-Aufforderungen, Ihr Passwort zu ändern, nie nach.

Sorgfaltspflicht

Ihr Arbeitgeber stellt Ihnen einen gut eingerichteten Arbeitsplatz zur Verfügung, der Ihnen die tägliche Arbeit erleichtern soll. Behandeln Sie die Geräte sorgfältig.
Wenn Sie Daten bearbeiten, dann sind Sie in Ihrem Bereich für die Einhaltung des Datenschutzes und für die Datensicherheit verantwortlich.
Fragen Sie den ServiceDesk der Dienststelle Informatik (DIIN), bevor Sie eine Aktion starten, bei der Sie sich in irgendeinem Punkt nicht sicher sind.

Informationen und Kontakt

Bei Fragen zur Informatiksicherheit
Wenden Sie sich an die Organisations- und Informatikbeauftragten.

Für allgemeine Informatikfragen und für die Meldung von verdächtigen Vorfällen
Wenden Sie sich an den ServiceDesk der DIIN
servicedesk@lu.ch, 041 228 69 99

Internet
Aktuelle Informationen zum Thema Informatiksicherheit finden Sie im Intranet unter
www.informatik.lu.ch > intern > Informatiksicherheit

Gesetzliche Grundlage
Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz (SRL Nr. 26c)

KANTON LUZERN

Organisations- und Informatikbeauftragte

März 2014/900361

LUZERN

Informatiksicherheit

Merkblatt für den Alltag und weiterführende Hinweise

KANTON LUZERN

Liebe Mitarbeiterinnen und Mitarbeiter

Der Einsatz von PC, Notebook und anderen Informations- und Kommunikationsmitteln ist für uns alle selbstverständlich. Er birgt aber auch Risiken.
Ihr Sicherheitsbewusstsein und Ihr verantwortungsvolles Verhalten ist die wichtigste Voraussetzung, um diese Risiken gering zu halten.
Dieser Flyer soll Ihnen helfen, Risiken zu erkennen und richtig damit umzugehen.

Ihre Organisations- und Informatikbeauftragten

Passwort

Es ist wichtig, sichere Passwörter zu wählen, weil sie die Schlüssel zu Ihren persönlichen Daten sind. Gelingt es einem **Hacker**, Ihr Passwort zu knacken, kann er auf alle Systeme zugreifen, auf die Sie Zugriff haben. Zudem kann er sich damit als Sie ausgeben (sogenannter Identitätsdiebstahl).

Das Wichtigste in Kürze

- ☐ Geben Sie Ihre Passwörter weder Mitarbeitenden noch Stellvertretungen noch Systemverantwortlichen bekannt.
- ☐ Wechseln Sie Initialpasswörter nach dem ersten Gebrauch.
- ☐ Ändern Sie Passwörter regelmässig und wechseln Sie sie sofort bei Verdacht auf Missbrauch.
- ☐ Benutzen Sie verschiedene Passwörter für unterschiedliche Anwendungen.
- ☐ Schreiben Sie Passwörter am besten gar nicht auf oder nur an einem geschützten Ort.
- ☐ Speichern Sie keine Passwörter für die automatische Anmeldung.
- ☐ Benutzen Sie für das Passwort GROSS- und klein-Buchstaben, Sonderzeichen und Zahlen.

Tipp
Am einfachsten kann ein starkes Passwort mit Hilfe eines Satzes gebildet werden:

Satz: Luzern gewinnt 2 zu 1 gegen Basel!
Passwort: LUg2:1gB!

Umgang mit Informationen

Geschäftliche Informationen, die Sie an Ihrem Arbeitsplatz bearbeiten, dürfen nur berechtigten Personen zugänglich sein. Zeigen Sie auch auf dem Arbeitsweg, in der Freizeit (z. B. im Zug oder im Restaurant) und bei Gesprächen mit Freunden und Dritten die nötige Zurückhaltung, wenn es um **interne Angelegenheiten** des Kantons / des Arbeitgebers geht.

Das Wichtigste in Kürze

- ☐ Aktivieren Sie beim Verlassen Ihres Arbeitsplatzes konsequent die Bildschirmsperre → [Windows-Taste] + [L] gleichzeitig drücken.
- ☐ Holen Sie ausgedruckte vertrauliche Informationen umgehend beim Drucker ab.
- ☐ Entfernen Sie im Sitzungszimmer Flipchart-Blätter mit vertraulichen Informationen.
- ☐ Melden Sie sich bei Arbeitsschluss vom internen Netzwerk ab.
- ☐ Schliessen Sie vertrauliche Akten und Datenträger (DVDs, USB-Sticks) ein.
- ☐ Werfen Sie vertrauliche Papierdokumente nicht ins Altpapier, sondern schreddern Sie sie.
- ☐ Verifizieren Sie die Identität von Anrufenden bei Telefonauskünften zum Beispiel über einen Rückruf oder die Abfrage von Informationen, die nur die betreffende Person wissen kann.

Mobile Geräte

Ob mit Smartphones oder mit Tablet-PCs, fast sämtliche Funktionen eines PC können auch mobil genutzt werden. Wegen ihrer geringen Grösse können sie aber auch leichter **verloren** gehen oder **gestohlen** werden.
Mit dem Austausch sensibler Daten über mobile Geräte tritt auch deren Sicherheit vermehrt in den Fokus. Für die Sicherheit der Smartphones und Tablet-PCs gilt das Gleiche wie für herkömmliche PCs.

Das Wichtigste in Kürze

- ☐ Schützen Sie Ihr Smartphone mit einem Passwort aus 4 bis 6 Ziffern. Vermeiden Sie einfache Zahlenreihen wie 1111 oder 123456.
- ☐ Aktivieren Sie die automatische Sperre, die sich bei Nichtgebrauch des Smartphones selbständig einschaltet.
- ☐ Lassen Sie Ihre SIM-Karte sofort sperren, wenn Sie Ihr Smartphone verlieren oder es gestohlen wurde.
- ☐ WLAN- und Bluetooth-Empfang lassen Sie am besten nur dann eingeschaltet, wenn Sie diesen benötigen – denn diese Netze bergen ein erhöhtes Sicherheitsrisiko. Mit dem Ausschalten schonen Sie ausserdem Ihren Akku und verlängern die Betriebszeit Ihres Gerätes.