Spar- und Leihkasse Frutigen

Die SLF schreibt Sicherheit GROSS

Sorgfältiger Umgang mit persönlichen Daten, sichere Passwörter, keine Links in Mails von Unbekannten aktivieren, den Virenschutz aktualisieren: All das sollte selbstverständlich sein. Doch reicht es aus? Die SLF will auch beim Digital Banking Verantwortung wahrnehmen und über Gefahren aufklären.

Cybercrime oder Kriminalität im Netz gehört leider zum Alltag. Raffiniert vermitteln Täter den Eindruck, dass man es mit einem bekannten Unternehmen zu tun hat.

Enkeltrick und Online-Betrug

Was der «Enkeltrick» am Telefon ist, ist die Cyberkriminalität im Netz. Dubiose Mails lesen sich in etwa so: «Sie haben $ 50 000 000 gewonnen. Aktivieren Sie den Zugangscode!» Oder: «Sie wurden beim Besuch unsittlicher Webseiten beobachtet. Klicken Sie hier, um den Browserverlauf zu löschen.» Oder: «Das Paket wartet auf Ihre Anweisungen. Um die Lieferung abzuschliessen, klicken Sie auf ‹Bitte sofort zustellen›.»

«Nahezu alle Betrugsversuche könnten verhindert werden, wenn jeder aufmerksam und skeptisch ist.»

Internetbetrug hat verschiedene Gesichter:
Identitätsdiebstahl: Diebstahl von Namen, Adressen, AHV-Nummern oder Bankdaten, um so illegale Aktivitäten durchzuführen.
Online-Betrug: Menschen mit falschen Angaben oder Versprechen in die Falle locken und so an ihr Geld kommen.
Phishing: Mit gefälschten E-Mails, Webseiten oder SMS an Passwörter, Bankdaten, Kreditkarteninfos herankommen.
Cybermobbing: Mit Mails oder in sozialen Medien schikanieren, belästigen, bedrohen.
Hacking: Unbefugtes Eindringen in Computersysteme.
Ransomware: mit «Schadsoftware» (Malware) Lösegeld erpressen, bevor die erfolgte Blockierung von Daten oder Systemen wieder aufgehoben wird.
Distributed Denial of Service (DDoS)-Angriffe: Webseiten mit massiven Anfragen überfluten => Überlastung oder Totalausfall.
Dark Web: «versteckter» Bereich des Internets; Umschlagplatz für Drogen, Waffen, gestohlene Daten.

LINDA schützt

Kriminalität im Netz ist jederzeit und überall denkbar. Im Bereich des Zahlungsverkehrs unterschiedet man vier Arten von Cybercrime:
– Social Engineering oder «menschliche» Täuschungsmanöver
– Phishing oder betrügerisches Ausspionieren von Passwörtern oder persönlichen Daten
– Malware oder Schadprogramme
– CEO-Fraud oder CEO-Betrug (Anordnungen von angeblichen Managern).

Im Zusammenhang mit dem Internet ist Gutgläubigkeit tatsächlich fehl am Platz. Dass man zuerst einmal misstrauisch sein sollte, war kaum die Absicht von Tim Berners-Lee, der Ende 1989 am CERN in Genf das World Wide Web erfunden hatte. Sein Ziel, Informationen und Nutzer zu vernetzen, hat heute eine ganz andere Dimension erhalten.
Optisch und inhaltlich verblüffend «echte» E-Mails, WhatsApp-Nachrichten oder SMS gelten als beliebte Betrugsmasche. Allen gemeinsam ist der Inhalt, nämlich die Aufforderung zu einer bestimmten Handlung. Auf einen Link zu klicken oder Daten und Passwörter zu nennen: das kann sich rasch als «trojanisches Pferd» herausstellen. Vorsicht!

Kluge Köpfe schützen sich

6 Regeln zum sicheren Passwort
– mindestens 12 Zeichen
– Ziffern, Gross- und Kleinbuchstaben, Sonderzeichen
– keine Tastaturfolgen wie «asdfgh» oder «45678»
– Passwörter sollten keinen Sinn ergeben und in keinem Wörterbuch vorkommen
– überall ein anderes Passwort nutzen
– Passwort verschlüsselt speichern

Digital Banking: Ein sicheres Passwort wählen und für sich behalten.
Unbekannte Nachrichten: Keine SMS, WhatsApp und E-Mails von Unbekannten öffnen.
Virenschutz: Das Antivirenprogramm laufend nutzen.
Zugriffsanfragen/Freigaben: Anfragen für Zugriff/Freigabe von Konten sorgfältig prüfen.
Unbekannte Kontakte: Kontaktversuche von Unbekannten ablehnen, Absender blockieren.

Eine gute Hilfestellung ist das Modell «LINDA» von card-security.ch:
Links, Anhänge von Unbekannten nie öffnen bzw. anklicken.
Inhalte von E-Mails prüfen.
Neutrale Anrede macht stutzig.
Dringlichkeit, Zeitdruck sind verdächtig.
Absender immer überprüfen.

Frutiger Anzeiger: Hätte ich alle Links mit Gewinnversprechen angeklickt, wäre ich längst ein gemachter Mann. Ich hatte nicht … War das gut?
Stefan Berger: Das war sehr gut. Oft reicht schon das Anklicken eines Links oder das Öffnen eines Dokuments, das Sie von einem unbekannten Absender erhalten. Beim Ausführen des Befehls zum Öffnen können bereits Programme auf Ihrem PC installiert werden, die Unberechtigten dabei helfen können, Ihre Aktionen auszuspionieren. So geben Sie im schlimmsten Fall preis, welche Passwörter Sie für welche Dienste nutzen.

Trickbetrüger werden immer gerissener, etwa mit «offiziellen» Logos von Behörden, Post, Banken. Woran erkennt man «gefakte» Mails?

Die SLF kümmert sich. Auch um Ihre Sicherheit bei digitalen Bankdienstleistungen.

Meist erkennt man über den Absender, ob es sich wirklich um den offiziellen Dienstleister oder um einen Fake handelt. Geprüft werden kann, ob die Mailadresse des Absenders wie ein privater Name oder ein scheinbar zufällig generierter Buchstabensalat aussieht, was eher für einen Betrugsversuch spricht – oder effektiv wie der Dienstleister, den man wirklich erwarten würde. Mittlerweile gibt es auch Dienste, die dabei helfen. Ein kostenloser Dienst ist flairsafe.ch. Dieser wird von verschiedenen offiziellen Stellen wie der Schweizerischen Kriminalprävention unterstützt. Dort kann mit der Weiterleitung der verdächtigen Mail oder dem Hochladen eines Screenshots innert weniger Sekunden geprüft werden, ob die Mail echt ist oder ein potenzielles Risiko darstellt. Am besten einfach mal versuchen!

Sie haben sich Sicherheit auf die Fahne geschrieben, gerade beim Digital Banking. Was ist Ihr Anspruch und wie setzen Sie ihn in die Praxis um?
Wir arbeiten mit dem aktuellen Sicherheitsstandard. Unsere Partner in den verschiedenen Lösungen tun dies ebenfalls. Sämtliche Produkte und Dienstleistungen werden laufend überprüft und gegebenenfalls optimiert, auch was die Sicherheit anbelangt. Zudem versuchen wir, unsere Kundschaft zu informieren und so präventiv Betrugsversuchen entgegenzuwirken. Auch hier gibt es kostenlose Portale für zuhause, etwa cybersecurityforyou.ch.

Bei Ihnen daheim. Ihre kompetente Regionalbank für alle finanziellen Bedürfnisse. Mit der Erfahrung seit 1837 – und trotzdem jung geblieben!

Hand aufs Herz: Ist absolute Sicherheit möglich?
Nein. Absolute Sicherheit gibt es so nicht. Das Handeln des schwächsten Glieds in der Kette – nämlich des Benutzers selbst – kann alle Sicherheitsvorkehrungen zunichtemachen. Dies ist das grösste Risiko. Zudem findet in der Betrugsbekämpfung ein Wettlauf statt. Betrug wird weltweit organisiert, Techniken werden ständig verfeinert. Auf der anderen Seite wird tagtäglich an der Prävention und an der Verhinderung dieser Verbrechen gearbeitet. Wichtig ist zu wissen, dass nahezu alle Betrugsversuche verhindert werden können, wenn man aufmerksam und skeptisch bleibt; also nicht einfach reagieren, wenn eine Anmeldemaske auf dem Bildschirm erscheint. Im Zweifelsfall kurz innehalten, eventuell bei jemand Vertrautem nachfragen: Macht das Sinn? Würdest du das auch so machen?

Hilfreiche Links

Weitere Informationen und Tipps finden Sie hier:
– www.ibarry.ch, Plattform für Internetsicherheit
– www.flairsafe.ch, Schweiz. Kriminalprävention
– ncsc.admin.ch/nscs/de/home.html, Bundesamt für Cybersicherheit
– www.card-security.ch/karte-schuetzen
www.cybercrimepolice.ch
www. cybersecurityforyou.ch
www.ebas.ch, www.s-u-p-e-r.ch

…und wenn trotzdem einmal etwas schiefgeht?
Wer auf Nummer sicher gehen will, kann vorgängig eine Versicherung abschliessen. Damit müssten die grössten Risiken abgedeckt sein.
Wenn es bereits zu spät ist, ist Handeln angesagt: sofort den Support kontaktieren und den Fall melden. Wir sperren im Hintergrund alle betroffenen Zahlungsmittel und sorgen dafür, dass alles andere normal weiterverwendet werden kann. Sämtliche Support-Nummern sind auf unserer Webseite ersichtlich.
Danach gilt es, wie bei jedem anderen Verbrechen auch, die Polizei zu kontaktieren und Anzeige zu erstatten.

Vielen Dank fürs Gespräch!
Interview: Thomas Feuz

Mehr erfahren:
Interessiert an einer Beratung rund um Geld und Sicherheit?
Hier gibt's ganz schnell mehr:

slfrutigen.ch/sicherheit

Zur Person

Stefan Berger
Bereichsleiter Bezahlen und Kundendaten
Seit 2007 bei der SLF tätig
Ausbildung: Dipl. Bankwirtschafter HF
Hobbys: Sport, Literatur, Kulinarik, Gaming; wohnt in Frutigen