TOP 10 CYBERSECURITY AWARENESS TOPICS

PHISHING

Halten Sie Ausschau nach Phishing-Mails!
Phishing ist ein Betrugsversuch, bei dem der Empfänger eine gefälschte elektronische Nachricht (E-Mail, SMS, usw.) erhält, diese aber oft zunächst nicht als solche erkennt. Diese Nachrichten sind so gestaltet, dass der Empfänger zur Preisgabe sensibler Daten verleitet werden soll. Die Angreifer bedienen sich dabei der Identität realer Unternehmen oder Institutionen als gefälschte Absender, um Sie zur Preisgabe dieser Informationen zu verleiten!

P@S$W*RTER

Nutzen Sie immer starke Passwörter! Starke Passwörter sind min. 10 Zeichen lang und enthalten Gross- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Passwörter dürfen nie für zwei Logins (z. B. Versandhändler und E-Mail-Account) verwendet werden.

RANSOMWARE

Ransomware ist eine Schadsoftware und wird auch «Verschlüsselungstrojaner» genannt. Diese bösartige Software verschlüsselt Dateien auf dem Mobilgerät oder auf dem Computer sowie auf den damit verbundenen Netzlaufwerken. Dem Opfer wird versprochen, dass die Daten nach der Bezahlung einer hohen Summe wieder entschlüsselt werden. Schützen Sie sich und seien Sie wachsam: Anhänge in E-Mails, unseriöse Webseiten, fremde USB-Sticks usw. können Ransomware enthalten!

MOBILE DATENTRÄGER

Mobile Datenträger wie USB-Sticks oder externe Festplatten sollten nicht verwendet werden. Falls doch, dann müssen diese immer sicher weggeschlossen und die Dateien darauf verschlüsselt werden. Um eine Datei auf einem USB-Stick oder auf einer externen Festplatte zu verschlüsseln, kann eine Software, z. B. das kostenlose Tool "7-Zip„, verwendet werden.

MOBILE PHONE

Auch ein Mobile Phone muss wie ein Computer vor Cyberkriminellen geschützt werden. Schützen Sie es entsprechend mit einem sicheren Passwort. Das Mobile Phone zu „rooten“ (Android) oder mit einem „Jailbreak“ (iPhone) zu versehen, kann die Sicherheit Ihres Mobile Phone markant beeinträchtigen.

WER HÖRT UND LIEST MIT?

Achten Sie darauf, wer mithört oder mitliest. Telefonate können bei einem offenen Fenster oder im Zug ganz einfach mitgehört werden! Achten Sie also darauf, wer Ihnen zuhört oder auf den Bildschirm sehen kann. Schon wenige Informationen von Ihrem Bildschirm (z. B. eine E-Mail) können einem Angreifer helfen, später einen Social Engineering-Angriff erfolgreich durchzuführen. Daher sollten Sie nicht in den öffentlichen Verkehrsmitteln arbeiten.

Social Engineering

Unter Social Engineering wird das Durchführen von Angriffen auf Informationen und Systeme unter Ausnutzung der «Schwachstelle Mensch» verstanden. Der Angreifer versucht an wichtige Informationen zu gelangen, indem er Sie mit psychologischen Tricks überlistet. Seien Sie wachsam bei jeder Konversation (persönlich, E-Mail, Telefon, usw.), in der Ihnen Fragen gestellt werden, welche ausserhalb des „Normalen“ liegen. Lassen Sie sich nicht unter Druck bringen, denn dies ist ein beliebter Trick von Angreifern. Lassen Sie sich Zeit - Sie müssen auch Fragen nicht immer direkt beantworten.

SICHERES SURFEN

Es ist wichtig, dass Sie nur sichere Webseiten verwenden. Seien sie skeptisch: Nichts ist gratis, auch nicht im Internet - im Zweifelsfall zahlen Sie mit Ihren Daten oder mit einer Malware-Infektion!

ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA)

Die Methode, zusätzlich zum Passwort eine zweite Sicherheitsprüfung zu durchlaufen, ist ein sicheres Mittel, um Ihr Konto gegen einen Cyber-Angriff zu schützen. Setzen Sie 2FA konsequent für den Zugriff auf sensitive Informationen ein. Der Einsatz von 2FA bei Ihrem E-Mail-Postfach oder auch bei Ihrer Dateiablage ist empfohlen.

***

HUMAN FIREWALL

Wir, die Menschen, tragen die Verantwortung, ob Kriminelle die Schwachstelle Mensch ausnutzen können: *Sie wählen ein sicheres Passwort! Sie lassen keine Dokumente unbeaufsichtigt liegen! Sie unterlassen es, im Zug zu telefonieren! Sie erkennen, dass es sich um eine Phishing-Mail handelt! Sie nutzen den gesunden Menschenverstand, bevor Sie einen Post auf LinkedIn oder Facebook machen! Sie verschlüsseln Ihre E-Mails und Dateien auf mobilen Datenträgern! Sie nutzen nur sichere Webseiten!*

SWISS INFOSEC

Swiss Infosec AG
Centralstrasse 8A
6210 Sursee

+41 41 984 12 12
infosec@infosec.ch
www.infosec.ch

Mehr erfahren:
Cybersecurity
Awareness