InfoGuard
SWISS CYBER SECURITY

ICT-SECURITY
LASS DICH NICHT TÄUSCHEN

ICT-SECURITY LASS DICH NICHT TÄUSCHEN

Merkblatt

InfoGuard AG

Schutz vor Phishing & Ransomware

- Überprüfe jedes E-Mail, bevor du weitere Aktionen ausführst.
    1. Prüfe die Absenderadresse; kennst du die Person?
    2. Passt der Betreff des E-Mails zum Absender?
    3. Wird im Mail versucht, dich zu einer Aktion zu bewegen, beispielsweise das Attachment zu öffnen, einen Link anzuklicken oder setzt man dich unter Zeitdruck, oder droht mit Konsequenzen usw.?
    4. Ist der Inhalt des Mails für dich plausibel?
    5. Prüfe jeden Link in einem Mail genau, aber ohne zu klicken! Wenn du mit dem Mauszeiger auf den Link fahren, welche URL wird angezeigt – entspricht diese dem angezeigten Link im Mail?
    6. Aktiviere auf keinen Fall die Makro-Funktion beim Öffnen von Office-Dateien.
    7. Lösche E-Mails direkt, bei denen du dir sicher bist, ohne den Anhang zu öffnen.
    8. Wenn du unsicher bist, sende das Mail per Anhang an unser HelpDesk xxx@xxxx.ch
- Ignoriere auf keinen Fall die Sicherheitswarnungen und aktiviere nur Makros aus vertrauenswürdigen Quellen
- Sei aufmerksam in Bezug auf psychische Manipulation: Situationen oder Nachrichten, welche die Neugier wecken sollen, übertrieben formuliert sind, Druck ausüben oder Eile erfordern, sei skeptisch.

ICT-SECURITY LASS DICH NICHT TÄUSCHEN

Merkblatt

InfoGuard AG

InfoGuard
SWISS CYBER SECURITY

Geben Sie Phishing-Mails keine Chance!

So entlarven Sie Cyberkriminelle

Datum

- Wurde die E-Mail zu einer ungewöhnlichen Uhrzeit geschickt (Nacht, Wochenende)?

Empfänger

- Wurde die E-Mail noch an andere Personen geschickt?
- Falls ja: Kennen Sie diese Personen? Sind es ungewöhnlich viele?

Betreff

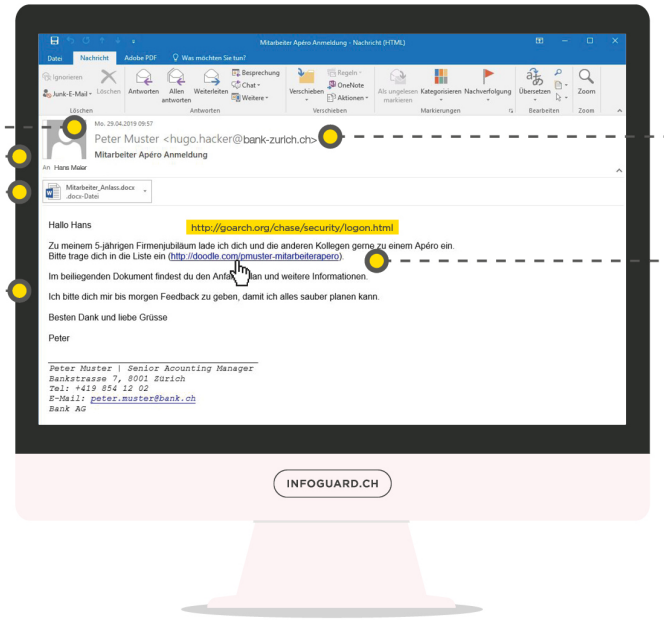
- Stimmt der Betreff mit dem Inhalt überein?
- Ist es eine Antwort auf eine E-Mail, die Sie geschickt oder angefordert haben?
- Ist der Betreff persönlich oder eher allgemein formuliert?

Anhang

- Erwarten Sie eine entsprechende Datei?
- Falls der Absender von intern stammt: Stimmt der Dateiname mit den bei Ihnen üblichen Bezeichnungen überein?
- Wirkt der Dateiname vertrauenswürdig?
- Ist es ein üblicher Dateityp?
- Hat der Virenscanner die Datei gemeldet?
- Beinhaltet das Dokument Makros? (Nicht aktivieren!)

Inhalt

- Ist die Ansprache unpersönlich?
- Wird eine Aktion von Ihnen verlangt (Herausgabe/Eingabe Logindaten, Zahlungsaufforderung etc.)?
- Wird mit Konsequenzen gedroht, beispielsweise bei Nichtreaktion (Geldverlust, Strafanzeige, Konto- oder Kartensperrung etc.)?
- Hat der Text Rechtschreib-/Grammatikfehler oder eine unübliche Formatierung?
- Sieht die Signatur/der Footer vertrauenswürdig aus?
- Werden verschiedene Schriftgrössen, -formatierungen, -farben etc. verwendet?



Absender

- Kennen Sie den Absender?
- Falls ja: Ist es dieselbe E-Mail-Adresse wie beim letzten E-Mail-Kontakt?
- Wurde die E-Mail von einem Bekannten, Partner oder Lieferanten geschickt, ist inhaltlich aber ungewöhnlich resp. uncharakteristisch?
- Stimmt die E-Mail-Adresse mit dem Anzeigenamen des Absenders überein? (Peter Muster → <hugo.hacker@bank-zurich.ch>)
- Handelt es sich bei der E-Mail-Adresse um eine gefälschte Domain? (@bank-zurich.ch → @bank.ch)

Hyperlinks

- Wenn Sie mit der Maus über den Link fahren (s. links in gelb): Wird dieselbe Zieladresse angezeigt? (Achtung: Auf keinen Fall klicken!)
- Ist der Link ungewöhnlich lang?
- Wird im Text Bezug zum Link genommen?
- Ist die Zieladresse des Hyperlinks fehlerfrei? (z.B. www.apple.com → www.appple.com)

Allgemeine Tipps

- Hören Sie auf Ihr Bauchgefühl: Wenn Sie nicht sicher sind, ob die E-Mail echt oder ein Betrug ist, lassen Sie sie lieber durch Ihr IT-Sicherheitsteam überprüfen.
- Klicken Sie bei Unsicherheiten niemals auf einen Link und öffnen Sie auf keinen Fall die Datei.
- Wenn Sie vermeintlich sichere Anhänge öffnen und eine Warnmeldung erscheint, lassen Sie die E-Mail durch Ihr IT-Sicherheitsteam überprüfen.
- Im Zweifelsfall in einer neuen, separaten E-Mail oder telefonisch beim Absender nachfragen, ob er oder sie tatsächlich diese E-Mail geschickt hat.

ICT-SECURITY LASS DICH NICHT TÄUSCHEN

Merkblatt

InfoGuard AG

InfoGuard
SWISS CYBER SECURITY

Sicherer Umgang mit Passwörtern

- Gib Passwörter nie an Dritte weiter.
- Benutze Passwörter niemals für mehrere Anwendungen.
- Ändere temporäre Passwörter oder Initial-Passwörter beim ersten Login.
- Verwende starke Passwörter bestehend aus mindestens 12 Zeichen (Zahlen, Gross- und Kleinbuchstaben sowie Sonderzeichen).
- Verwende nie einfach zu erratende Passworte wie Geburtstage, Namen oder Begriffe aus dem Wörterbuch.
- Nutze einen Passwortmanager (z.B. KeePass).
- Aktiviere (falls vorhanden) die Zwei-Faktor-Authentifizierung.
- Speichere Passwörter nie in einer Anwendung (beispielsweise im Internet-Browser), insbesondere nicht um automatisch angemeldet zu bleiben. Lösche daher in deinen Browser-Einstellungen regelmässig die Option «Autovervollständigung».

ICT-SECURITY LASS DICH NICHT TÄUSCHEN

Merkblatt

InfoGuard AG

InfoGuard
SWISS CYBER SECURITY

Persönlicher Grundschutz gilt auch im Home Office

- Aktualisieren Sie Ihre Software und OS regelmässig.
- Sichern Sie Ihre Daten regelmässig mit Backups
- Nutzen Sie ein Antivirus-Programm mit Webfilter und halten Sie dieses aktuell
- Schützen Sie Ihren Internetzugang mit einer Personal-Firewall
- Verwenden Sie starke und unterschiedliche Passwörter oder wenn möglich sogar eine Zwei-Faktor-Authentisierung
- Ignorieren Sie NICHT die Sicherheitswarnungen und aktivieren Sie keine Makros.

Melde Vorfälle

- Solltest du Fragen haben oder etwas Ungewöhnliches bemerken, melde dich bitte unverzüglich beim HelpDesk: **xxx@xxxx.ch / Telefon**