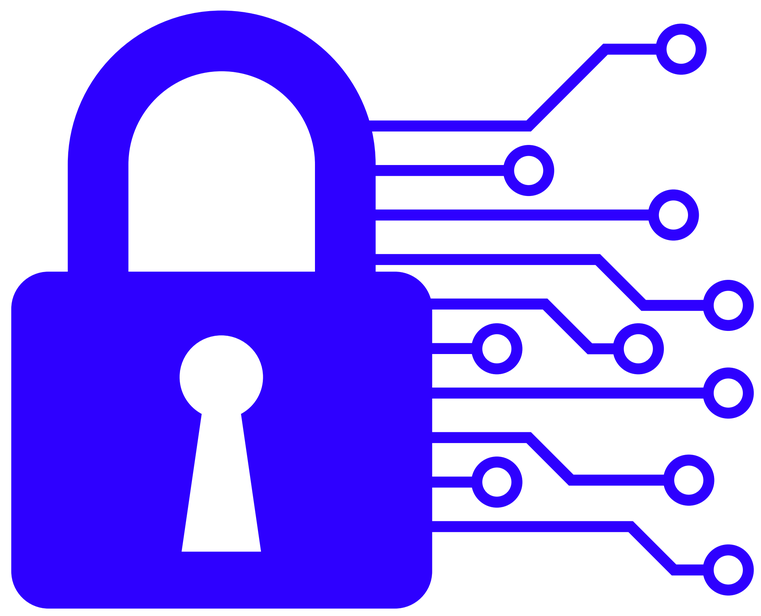
مصرف الراجحي
alrajhi bank

نصائح للبقاء آمنًا ضد الإحتيال

مع تزايد تطور وهجمات الانترنت، من الضروري البقاء متقدمين على مجرمي الانترنت.هذه الاقتراحات حيويه لحماية بياناتك، خاصه خلال الحالات الحرجه.

١- كن يقظًا تجاه رسائل البريد الالكتروني الاحتيالية والمكالمات الهاتفية المزيفة.

- كن حذرًا من الاستفسارات الغريبه او العاجله التي تصلك عبر البريد الالكتروني.
- انتبه من المكالمات الهاتفيه المزيفه او المشبوهه، لا تشارك اي معلومات عبر الهاتف إذا كنت غير متأكد من صحة الشخص المتصل بك.
- قم بتأكيد صحة الطلب قبل الكشف عن اي معلومات لأطراف غير مألوفه.
- تجنب النقر على الروابط او تنزيل المرفقات إذا كنت شاكًا بصحة المرسل.



2 - كن آمنًا أثناء تصفح الإنترنت.

- قم بزيارة مواقع الويب الموثوقة فقط وأضفها إلى المفضلة. الموقع الآمن يبدأ بـ "https" حيث يشير الحرف "s" إلى الأمان. فإن البيانات المتبادلة مع الموقع لا يمكن التقاطها أو تعديلها.
- استخدم التوثيق المتعدد عندما يكون ذلك ممكنًا،في حال عدم توفر ذلك، استخدم كلمات مرور فريدة.
- استشر مصادر معروفة وذات سمعة جيدة فقط للحصول على أحدث الأخبار العالمية وتبرع من خلال القنوات الرسمية فقط.

٣ - كن حذرًا من شبكات الواي فاي العامة والتنزيلات.

- كن حذرًا من نقاط الواي فاي العامة. تجنب استخدامها للأمور المصرفية عبر الإنترنت، أو البريد الإلكتروني، أو تحديث وسائل التواصل الاجتماعي، حيث يمكن للمخترقين الوصول إلى معلوماتك.
- قم بتنزيل البرامج فقط من متاجر التطبيقات الموثوقة وحافظ على تحديثها بانتظام.

4 - كن حذرًا فيما تشاركه.

- انتبه من ما تشاركه وتعجب به على وسائل التواصل الاجتماعي.
- تجنب نشر (أو تضمينه في ملفك الشخصي العام) معلومات شخصية مثل تاريخ ميلادك، عنوان منزلك، معلومات الاتصال، تواجدك خلال عطلتك، وأية معلومات أخرى يمكن استغلالها من قبل المجرمين.
- أضف فقط الأشخاص الذين تعرفهم إلى شبكتك واستخدم إعدادات الخصوصية لتقييد من يمكنه رؤية ما تشاركه.

٥ - توقف. فكر. تصرف.

- توقف إذا كان هناك شيء غير صحيح.
- فكر في المخاطر.
- تصرف بشكل آمن في جميع تفاعلاتك الرقمية.

تذكر: مصرف الراجحي لا يتواصلون أبدًا مع العملاء عبر الهاتف أو البريد الإلكتروني أو الرسائل النصية لطلب اسم المستخدم وكلمة المرور أو معلومات الحساب أو كلمة المرور لمرة واحدة (OTP). كما أننا لا نرسل رسائل بريد إلكتروني تحتوي على روابط إلى صفحات تسجيل الدخول مثل الخدمات المصرفية عبر الإنترنت، أو أرقام العقود، أو الأرقام السرية (PINs).

مصرف الراجحي
alrajhi bank

Tips To Stay Fraud Safe

As cyber-attacks become increasingly advanced and frequent, it's crucial to stay ahead of cybercriminals. These suggestions are vital for safeguarding your data, especially during critical situations.

1 - Stay vigilant for fraudulent emails and fake phone calls.

- Be cautious of strange or urgent demands received via email, phone, or text message.
- Keep an eye out for fake or misrepresented calls.
- Never share information over the phone if you're uncertain about the caller's legitimacy.
- Confirm the validity of a request before disclosing any information to unfamiliar parties.
- Avoid clicking on links or downloading attachments if you're skeptical.

2 - Maintain a secure online presence.

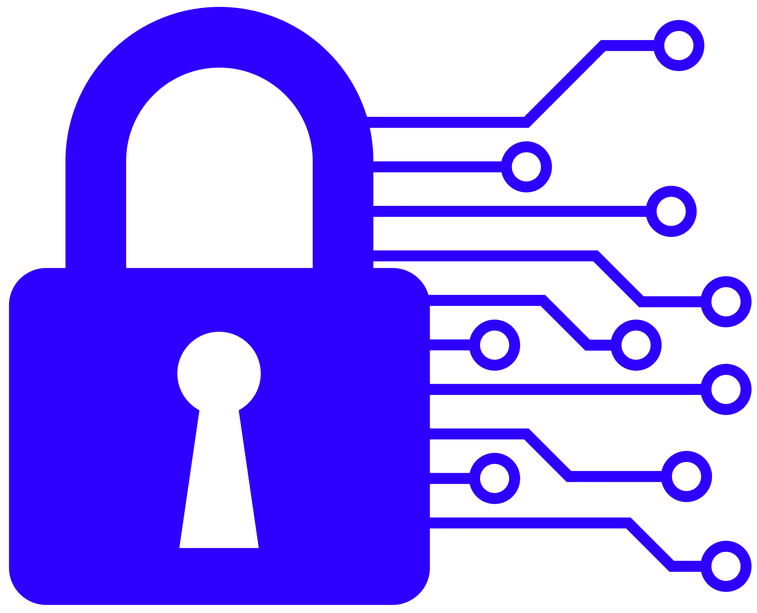
- Stick to visiting verified websites and consider bookmarking them. A secure site will start with "https://", where the "s" indicates security, making data exchange safe and unalterable.
- Utilize two-factor authentication when available, or alternatively, employ strong, unique passwords managed through a password manager.
- Rely only on well-known, credible sources for news updates and contribute only through official donation platforms.

3 - Exercise caution with public Wi-Fi and software downloads.

- Be skeptical of public Wi-Fi networks, steering clear of activities like online banking, email, or social media updates, as these could be compromised by hackers.
- Download apps exclusively from reputable app stores and ensure they are updated regularly.

4 - Be selective about your online interactions.

- Be cautious about what you like and disclose on social media platforms.
- Refrain from publicly sharing sensitive information like your birth date, residential address, contact info, or travel plans, as this can be used maliciously.
- Only connect with individuals you're familiar with, and use privacy settings to control what's visible to others.



5 - Pause. Reflect. Proceed.

- Pause if something appears off.
- Take secure actions in all your online activities.
- Consider the associated risks.

Remember: Alrajhi Bank never contacts clients via phone, email, or text to request username/password, account information, or one-time password (OTP). We also don't send emails containing links to login pages like e-banking, contract numbers, or PINs.