SCAN WITH CAUTION

What you should know about QR codes and convenience tech before you scan, tap, or check in

Educational Community
ALLIANCE CREDIT UNION

EDUCACU.COM | 419-381-2323
3845 Angola Road, Toledo, OH 43615

THIS MONTH'S TOPICS:

From QR code menus to digital boarding passes, convenience tech has become a routine part of daily life. But the more we rely on quick scans and automated devices, the easier it becomes for cybercriminals to hide behind them.

This month's newsletter looks at the overlooked risks built into the tools we use without thinking, and how small changes in awareness can prevent big security problems. As the holiday season ramps up and our schedules get busier, staying alert to these subtle threats is more important than ever. By understanding how these everyday tools can be manipulated, you'll be better prepared to spot red flags before trouble occurs.

QR CODE *DEEP DIVE*

What are QR codes and how are they used?

QR (Quick Response) codes are two-dimensional barcodes that link you directly to information, websites, or actions with a quick scan. Today, they're used everywhere: menus, boarding passes, parking meters, event tickets, retail returns, and more.

Common types of QR codes include URL codes (that open websites), Wi-Fi codes (connect your device to a network), payment codes (initiate transactions), app/download codes (link to app stores or files), and contact codes (save vCard details).

PROS ✓

- *Fast, contactless, and easy to use*
- *Store many types of information*
- *Cost-effective for businesses*
- *Reduce printing and manual*
- *entry errors*

CONS ✗

- *You can't see where a QR code leads until after scanning*
- *Easy for scammers to swap or cover with fake versions*
- *Can trigger automatic actions (Wi-Fi joins, downloads, messages)*
- *Increasingly used in phishing attacks ("quishing")*

How do cybercriminals exploit QR codes?

Attackers take advantage of how quickly people scan QR codes without checking their source. Common tactics include:

- **Fake stickers** placed over real QR codes at restaurants, parking meters, or event booths that lead to phishing sites or fake payment portals.
- **Malicious links** that steal login information, request credit card details, or trigger dangerous downloads.
- **Rogue Wi-Fi networks**, created by QR codes that automatically connect your device to an attacker-controlled hotspot.
- **Social engineering scams** using QR codes in fake delivery notices, parking tickets, event flyers, or donation requests.

BOARDING PASSES

What's hidden inside a boarding pass?

Boarding passes look simple, but their barcodes can reveal full name and date of travel, airline loyalty numbers, booking codes (PNR), itinerary details, frequent flyer account access points, passport information, emergency contacts, and special service notes.

How can attackers use boarding pass data?

- **Frequent Flyer Account Access:** Some airlines allow login using only a name + PNR number, making stolen miles and personal data easy to exploit.
- **Itinerary-Based Scams:** Attackers use your travel dates to send fake alerts like "Your flight has changed" or "Your upgrade request needs confirmation."
- **Identity Clues:** Paired with social media posts, boarding pass data helps criminals build detailed profiles for phishing or impersonation.
- **Reservation Manipulation:** In some systems, scammers can change seat selections, cancel flights, or view linked traveler details.
- **Location Tracking:** Travel patterns expose when you're away from home — valuable information for both cyber and physical crimes to take place.

How can you protect yourself?

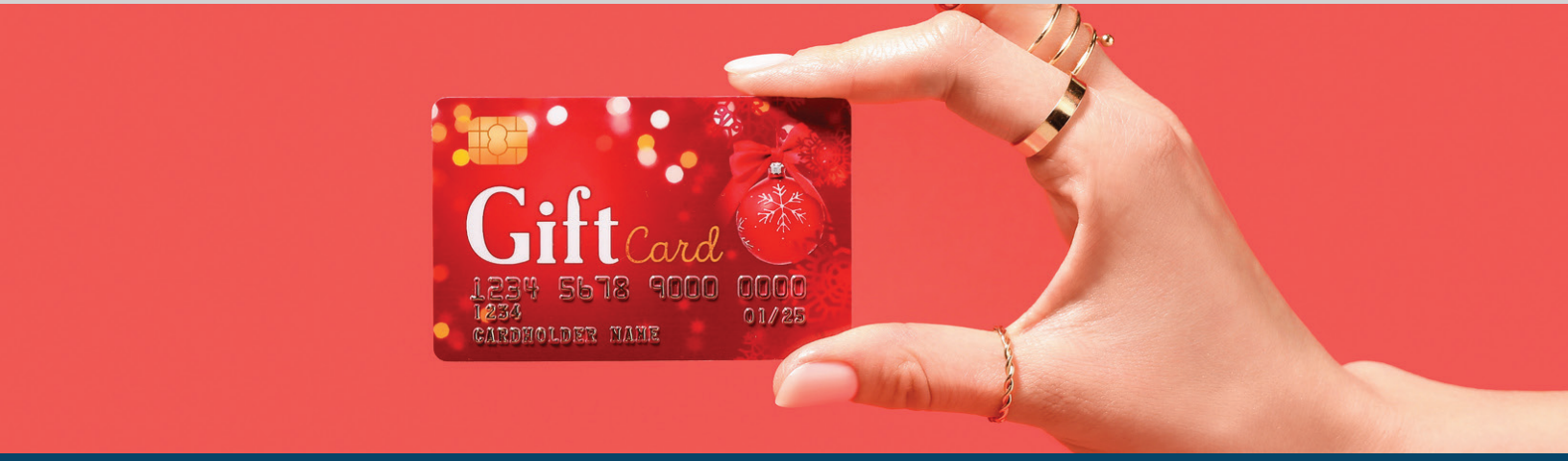
- Never post your boarding pass online, even if the barcode is partially blurred.
- Shred or tear boarding passes before throwing them away.
- Avoid leaving boarding passes in hotel rooms, rental cars, or seat pockets.
- Monitor frequent flyer accounts for unusual activity.
- Be suspicious of unsolicited flight-related messages, even if they reference real trip details.
- Use official airline apps rather than printed passes whenever possible.

SCAM OF THE MONTH: GIFT CARD SCAMS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Maya was rushing through her workday when an urgent email from her manager arrived: “I’m tied up in meetings. Please grab four $100 gift cards for a client and send the codes. Don’t call; I’m presenting.” The message came through at the perfect moment. Maya was juggling deadlines, responding to questions, and trying to finish urgent tasks. The email used the correct signature and carried the same tone her manager often used. She hurried to the store, bought the cards, and sent the codes as requested.

Later that afternoon, Maya mentioned the purchase to her real manager on a call, only to learn they had never sent the email. The truth set in: she’d been tricked by a gift card scammer impersonating her supervisor. By the time she contacted the store, the balances were already drained.



DID YOU SPOT THE RED FLAGS?

- A request that says “Don’t call me” or discourages verification is a major warning sign of impersonation or fraud.
- Any urgent demand for gift cards, especially paired with pressure to act quickly, is a classic scam tactic.

HOW TO PROTECT YOURSELF

- If an email asks for gift cards, money, or urgent action, confirm the request with the person directly.
- If you receive an urgent request that seems suspicious while you’re juggling multiple tasks, pause before you act.

EVERYDAY CONVENICE TECH

What We Use Without Thinking

Tap-to-Pay Tools

- Mobile wallets
- Contactless card readers
- NFC-enabled devices

Digital Touchpoints

- QR menus & payment codes
- Package pickup lockers
- Online return portals

Smart Features

- Auto-connect Wi-Fi
- Bluetooth accessories
- Public charging stations

How Attackers Take Advantage

Tampered Technology

- Fake QR code stickers on menus, parking meters, or kiosks
- Altered checkout terminals that reroute payments

Automatic Connections

- Devices linking to rogue Wi-Fi networks
- Bluetooth pairing requests disguised as notifications

Data Harvesting

- Malicious apps installed through quick-scan codes
- Tracking via “free” convenience tools
- Screenshots and digital passes revealing travel or personal info

Smarter Ways to Use Convenience Tech

- Look for tampering (misaligned stickers, poor print quality)
- Only scan codes from trusted sources
- Turn off Bluetooth & auto-connect when not in use
- Use personal hotspots instead of public Wi-Fi
- Use official apps for returns, payments, and loyalty programs
- Keep OS and apps updated