Cyberattack case studies: what scams are out there and what you can do.

Cybercriminals are getting more and more creative. They're adapting their tricks to match how we live, work, and connect online. What used to be obvious spam emails have evolved into sophisticated schemes that can fool even the most cautious users. To help you stay a step ahead, we're looking at four cyberattack case studies from KnowBe4 and what you can do to protect yourself.

Cyberattack case study #1: QR code confusion.

In this ploy, scammers deliver packages to homes that didn't order anything with QR codes on the labels. The idea behind the scam is that confused recipients will scan the code to find out what this package contains and who it's from. The codes then take users to fake websites where they're asked to enter their personal information. But really, it's all a plot to secretly install malware on your device.

How to avoid it:

- Look at any unexpected packages or mail critically before opening or interacting with them.
- Never scan QR codes from sources you don't recognize.

Cyberattack case study #2: Travel malvertising.

In this travel-related scam, cybercriminals target travelers with online advertisements. Let's say you book a trip abroad and have questions about your reservation. Cybercriminals add false customer service numbers or deals to search results to entice callers. Once on the phone, they may try to pitch you a better

rate and ask for your credit card information to book the false deal.

How to avoid it:

- Be wary of deals that are suspiciously low or too good to be true.
- Look at ads with a critical eye before clicking or calling.
- Only call phone numbers from your initial online confirmation or directly from the trusted company's website.

Cyberattack case study #3: False traffic fines.

Have you ever received a text message saying you've neglected to pay a traffic fine or toll? These messages often come with threats of suspended licenses or jail time. In reality, this is a growing scam trying to get worried consumers to click links and pay false fines right into their pockets.

How to avoid it:

- Be alert to text messages asking for money that also prey on fear or urgency.
- If you have questions about a fine, go directly to your local motor vehicle office or call their verified phone number.

Cyberattack case study #4: Job seeker scamming.

When searching for jobs on online platforms, have you ever come across one that has too high a salary or feels too perfect? If you've applied, the hiring manager may respond to your application and ask you to click a link to confirm your direct deposit information — then to share information like your credit card, Social Security number, and home address. This job was likely entirely fake from the start and an attempt by scammers to catch vulnerable job seekers.

How to avoid it:

- Trust your gut. If a job listing feels off, it likely is.
- Don't provide any personal information before verifying the source asking for it. Look at the hiring manager's email and contact number to ensure they're affiliated with the company they claim to be.

When it comes to online crime, these cyberattack case studies only scratch the surface. The best defense to keep your information protected is being smart and skeptical, clicking cautiously, and staying informed of the latest tactics. For more support and peace of mind, talk to a local, independent agent today.

blog content is not intended to serve as professional or expert advice for your insurance needs. Contact your local, independent insurance agent for coverage advice and policy services.