# Quishing and vishing: How to protect yourself from new security threats

By Florian Kastner, pcworld.com, MAY 10, 2024

Quishing and vishing use modern technologies to obtain your data. Find out how you can protect yourself against these fraud methods.

In the ongoing battle against cybercrime, we are constantly coming across new methods that fraudsters use to try and obtain our sensitive data. While vishing is already a well-known threat, quishing is an even newer and more sophisticated method. Read on to find out what these terms mean and how you can protect yourself.

## What is vishing?

Vishing is a combination of the words “voice” and “phishing” and refers to fraudulent activities in telecommunications. The perpetrators pretend to be trustworthy persons or organizations in order to obtain sensitive data such as bank account information, credit card details, or passwords. Like many other scams, vishing falls under the heading of social engineering.

## How to recognize vishing

Typical signs of vishing are calls requesting urgent action or contact from organizations that you do not normally interact with.

For example, the caller claims to be an employee of your bank and says that there’s a problem with your account. You may be asked to provide your account information or credit card details in order to resolve the problem. The caller may also threaten you with consequences such as freezing your account or other penalties if you do not cooperate.

In other cases, fraudsters pretend to be Microsoft technicians after secretly infecting and locking the victim’s computer via a malware link. The person called is asked to pay for the repair or to purchase special software.

The so-called “police officer tactic” is also widespread. The perpetrators slip into the role of police officers and warn older people in particular about criminal gangs. They then urge the victims to hand over their valuables and cash reserves to the supposed “police” for safekeeping.

## Quishing: Fraud scam via QR codes

Quishing is the latest phenomenon in cybercrime and is proving to be particularly insidious. This method uses QR codes to lure users to fake websites where attempts are then made to obtain their data. The prevalence and ease of use of QR codes in everyday life make quishing a serious threat.

### How does quishing work?

Quishing attacks skillfully exploit the increasing interconnectedness of our digital environment. As it becomes more common to combine different devices and platforms for everyday tasks such as bank transfers, users are used to switching between their devices — from computer to smartphone, for example.

Cybercriminals are capitalizing on this habit by sending fraudulent emails pointing out a supposed security problem or claiming that the user urgently needs to download a document, accessible by scanning a QR code with their smartphone.

The devious intention is that users are directed to a fake website that is not recognized as such by smartphones. Two things can happen there: Either users download malware-infected documents or they enter their login details, which are then forwarded directly to the fraudsters.

# Protective measures against vishing and quishing

Cyber criminals are learning and becoming ever more cunning. People affected often find it difficult to assess the case and react calmly, especially if they are threatened with penalties or other consequences. Here are some important measures you can take against vishing and quishing.

### Protect against vishing:

- Ask for the name and location of the person calling you and make a note of this information. Then call the official phone number of the organization from which the call is supposedly coming to verify the identity of the caller.
- Do not give out any personal or financial information over the phone unless you have verified the caller's identity and are sure it's a legitimate enquiry.
- You can block unwanted calls from known scammers or suspicious numbers with call protection. The FCC provides a list of tools and resources to help.

### Protection against quishing:

- Be careful when scanning QR codes, especially if they come from an unknown or insecure source. If the message seems strange to you, we advise you to contact the supposed sender via official channels.
- Check the URL to which the QR code leads before entering any personal information. Reputable sites use encrypted connections (https).
- Activate multi-factor authentication for your online accounts. This provides an extra layer of security because even if fraudsters get hold of your login details, they will still need the second or third authentication factor to log in on your behalf.

# Conclusion

Both vishing and quishing are serious threats that cybercriminals skillfully use to gain access to your personal and financial data. By being aware of the specific tactics and warning signs associated with these scams and taking appropriate protective measures, you can effectively defend yourself.

Always be vigilant, avoid giving out sensitive information, whether over the phone or by carelessly scanning QR codes, and take the time to check the credibility of sources. Your security and the protection of your data should always come first.

*This article was translated from German to English and originally appeared on pcwelt.de.*