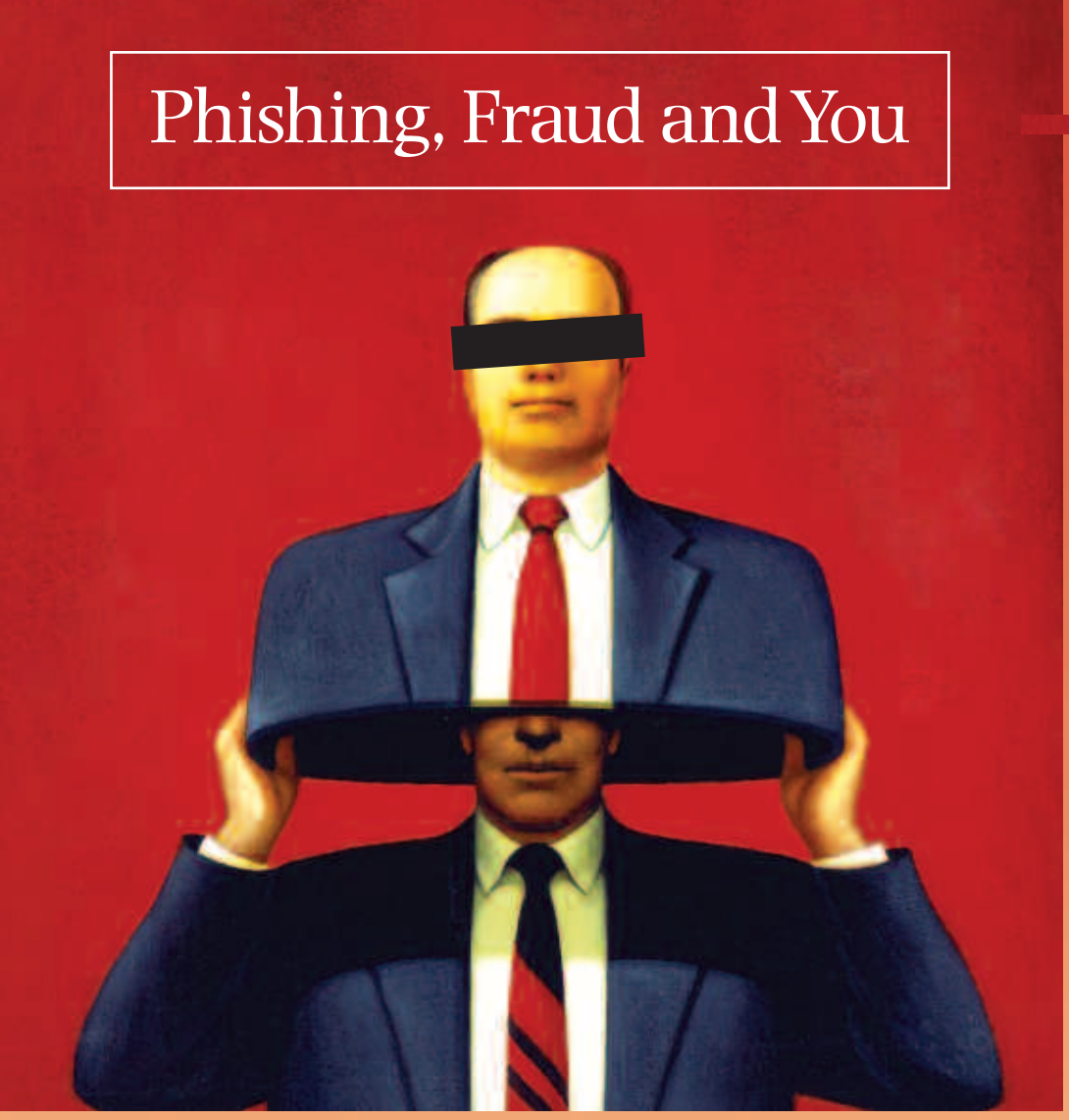
# Phishing, Fraud and You



## THESE DAYS, SCAMS ARE EVERYWHERE.

Identification theft, check fraud, online thievery ... if you can imagine it, there's a good possibility someone is doing it right now. True, the crooks seem to be getting more sophisticated, but the good news is there are ways you can protect yourself.

**Remember, knowledge is power. Here's your arsenal:**

### The Phone Call

It starts innocently enough. You get a phone call from someone claiming to be from your financial institution or credit card company asking you to verify some information. The scary thing is, the information they're asking for might not even seem important. Don't do it. For example, say the caller asks you to read off the last three numbers that appear on the back on your card near your signature strip. Seems simple enough. Again, don't do it. Those innocent little numbers are your unique "card verification value," and if a con artist already has your card number, they can use this information to convince online and phone merchants that they're you.

So how do you know which calls are real and which are fake? The clue is that the caller is asking you for personal data. If you ever get such a request, be suspicious. Just tell them that you don't discuss your financial account information over the phone and say you'll call back. If the call is legit, they'll understand. When you call back, make sure to call your financial institution directly or dial the 800 number on your credit card. Under no circumstances call a number provided to you by the caller.

### The Email

This is a really insidious one. Electronic messaging has made the con artist's life easier. Now they can target a large number of people in one shot thanks to a type of scam known as "phishing." Con artists send emails pretending to be a financial institution or company that you trust, often asking you to visit a website where you should validate your account/card information and establish a password.

The emails may mention that your account needs to be updated, or that you need to correct a problem on your account or advise you that you've been automatically entered into a program associated with your account or credit card. The goal is always the same – to get you to submit personal data that can be used for fraud or identity theft.

### The Pop-Up

Keep in mind that phishing is not confined to email, but can also be found on the Internet. Those fraudulent emails need websites where you can hand over your personal information. And these sites look very, very real.

Beware of pop-up screens asking you to verify information on a site you may be browsing. Be careful – it might not be associated at all with the original screen you were viewing. In the pop-ups, you're prompted to update banking and credit card account numbers and passwords. Don't do it. See a theme here?

### What You SHOULD Do

All the communications mentioned in this article have the potential to be fraudulent. The safest course of action is to not respond to any asking you to provide any personal or account information.

If you are suspicious about a site ... simply enter a wrong password. If the system lets you in ... chances are you've been diverted to a bogus site. If you're suspicious of a phone call, call back on a number you can verify before giving up your information. Remember, they can't do anything unless you give them what they want.

For more information on fraud scams, visit the Federal Trade Commission website at **www.consumer.gov/idtheft**, which is a national resource for information about identity theft.