Here's how to protect your mobile phone

David P. Willis, @dpwillis732 Published 6:00 a.m. ET July 21, 2017

Robocalls, telemarketers, and scams blowing up your smartphone can be very annoying. But what you can do about it? Democrat files

(Photo: BrianAJackson, Getty Images/iStockphoto)

Chalk it up to a weak moment.

Press on Your Side likes deals and discounts. Who doesn't? But recently, we signed up to receive coupons from a favorite store via text message.

When the first one dinged in, we realized we made a mistake. The text message and the link to the coupon were legitimate. But it left some worries.

More: Press on Your Side can teach you to fight scams

More: Ransomware: How to fight it

Will we be getting text offers from companies we don't want them from? Will scammers send fake offers and links via text message too? Did we just open the floodgates?

"It's very hard to think in advance, especially when you are given an incentive to give something away," said Janne Lindqvist, an assistant professor of electrical and computer engineering at Rutgers University in New Brunswick.

In this case, we had given away our cell phone number to a marketer.

"It might be several months later that I am on a list and might get some more targeted advertisements," said Lindqvist, who directs the Rutgers Human-Computer and Security Laboratory. "You make a decision today and the consequences will show up later."

And Press on Your Side was in the midst of preparing a column on keeping your mobile phone secure. Looks like we all need a refresher course.

1. Keep your cell phone number to yourself. "The new Social Security number … is your cell number," said Thomas Martin, president of Martin Investigative Services and author of "Seeing Life Through Private Eyes." Your smartphone "is a gateway to your living room to your bedroom, to your life."

2. Beware of text messages. Scammers may send text messages that look as if they come from a legitimate source, like a bank, a practice known as smishing. It could be an offer for a coupon, a free gift card, or a text that says you won a prize.

"The wording can be pretty much anything," Lindqvist said. "Treat everything with suspicion especially if it seems surprising or too good to be true."

The link could direct you to a website where you'll be tricked to share your personal information or one that can install malware on your phone. A hacker can try to encourage you to download an application that can compromise your phone.

"Never, ever click on a text," Martin said.

Hacker touching a smartphone screen, isolated on white background *(Photo: CreativaImages, Getty Images/iStockphoto)*

3. Make sure you update your phone's operating system. it will make it harder for a hacker to exploit your smartphone's software. "Attackers just need to find one way in," Lindqvist said. "It could be malicious apps that are exploiting a vulnerability that hasn't been patched yet."

Once opened, a hacker could read text messages and emails, have access to passwords or take over your mobile phone, Lindqvist said.

4.Protect your smartphone with a passcode. (And don't make it something unsecured, like 12345678.) "You should make sure if someone steals your phone, they can't unlock it right away," Lindqvist said.

More: Lakewood Welfare fraud: 5 reasons it's hard for the poor to do

5. Activate your smartphone's tracker, such as Find My Phone. and the ability to wipe your phone remotely. If someone takes it, you'll have a way to track it down or nuke your data.

6. Control your risk. Press on Your Side didn't need to share a mobile phone number. Lindqvist only uses his cell phone to make calls or send texts. "I am working on the assumption that I will lose it," he said.

Do you have a consumer problem that needs solving? Contact David P. Willis at 732-643-4042, pressonyourside@gannettnj.com or facebook.com/dpwillis732.