How a Phone is Phished: How to Safely Browse the Web and Avoid Attacks

What Do You Use Your Mobile Phone For?

Nearly 7 in 10 U.S. adults access the web via their mobile phones.

1 in 2
- U.S. adults check personal email on mobile phones
  - 25% once per week or less
  - 11% 2-5 times per week
  - 12% 1-2 times daily
  - 10% 4+ times daily

Is Your Mobile Phone Safe?

Mobile devices are the first systems to receive fraudulent email messages.

Most frequently emails call for immediate action, so mobile users are more likely to be hit by phishing attacks.

The first few words are the most important because after that, the site is taken down or caught by filters. Mobile users are usually the first to click.

Mobile Phishing Attacks Are More Frequent Than You Think

1 in 11
- U.S. users accessing phishing sites are more likely to submit their info on mobile than on desktop.

More people are likely to submit their info on mobile than on desktop.

The phishing site is hosted on a mobile device.


Phishing attacks per month, Dec 2010 - May 2011

Government and IRS & Tax Scams

- Government officials will not call you out of the blue.
- Government officials will not ask for personal information.
- Government officials will not threaten you with arrest.

Donations to Charities

- Japanese earthquake relief
- Donations to charity are fake, and they are not going to the people whom you want to give.

Various Social Network Phishing Scams

- Facebook users have been hit with phishing attacks.
- Phishing attacks often involve changing passwords or asking for personal information.

Tips to Stay Safe from Phishing on Your Phone

Email and URL:
- Be wary of emails or links to websites that do not look secure.
- Check if the URL is secure.

Check it out to make sure:
- Check the URL.
- Check the site's security certificate.
- Check the site's security certificate.

HTTPS:
- Use HTTPS.
- Use secure websites.
- Use secure websites.

Source: Lookout Mobile Security