PHISHING HAS MOVED TO MOBILE

What are the different tactics cybercriminals use and how can you protect yourself from it?

These days, everyone has a mobile device. We play and work in it, and for most employees, using their smartphone for both work and personal life is far more convenient. However, cybercriminals are also catching up with our dependability to our mobile device.

IPSYSTEMS,INC.
ALL ABOUT DATA SECURITY

Mobile phishing is now on the rise. In fact, it extends beyond email, SMS, and social media apps. Attacks are technically simple but seek to exploit human trust. For example, would you hesitate to click on a message saying that your loved one has been on an accident?

So what tactics do these attackers use?

1 URL PADDING

Is a technique that includes a real domain, however it's filled with dashes to hide the real destination which is usually a malicious site. Tiny URLs or shortened URLs are also used for this.

A padded URL would look like this: *http://m.facebook.com----------------validate----step1.rickytaylk[dot]com/sign_in.html*

2 SCREEN OVERLAYS

This type of phishing is designed to replicate a login page of a legitimate mobile app installed in your phone in order to capture your credentials. It is often deployed to use in scams and has shown to be highly effective; that is why it is a lucrative technique for hackers who are targeting mobile banking or online payment apps.

3 MOBILE VERIFICATION

Although this is a standard for all legitimate transactions online, attackers can also embed this authentication type to their phishing sites. This helps them identify that the device accessing their malicious site is indeed a mobile before they launch an attack.

4 SMS SPOOFING

Uses over-the-air (OTA) provisioning, this attack sends a fake text message to a user w/ a link and tricks them into clicking it. These messages often look like an update notification, but once clicked, it can intercept your email and web traffic.

How can you protect yourself from mobile phishing?

- Look for poor grammar and mispellings
- Be wary of offers that are too good to be true
- Call your bank about account suspensions or closings
- Ensure that your accounts keep up with new privacy settings
- Refrain from using public Wi-Fi networks
- Never click on suspicious looking links

Let's work together to fight phishing!

☎ +63 (2) 8638 - 3264
✉ inquiry@ipsystems.ph
🌐 www.ipsystems.ph

IPSYSTEMS,INC.
ALL ABOUT DATA SECURITY