

A close-up photograph of a computer keyboard. The central focus is a key with the word "Phishing" printed in bold red letters. To the right of the keyboard, a large, black, stylized '@' symbol is superimposed on the light blue background. A metallic, coiled cable or wire is draped over the "Phishing" key and extends towards the '@' symbol. Other keys visible include a bracket key to the left and a "Shift" key below.

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

[illegible]

1. תהליך המעבר מ-Android ל-iOS יתבצע באופן אוטומטי, אך יש צורך בהתקנת תוכנת המעבר (Transfer) על המחשב. תוכנת המעבר תאפשר למשתמש להעביר את כל הנתונים שלו, כולל תמונות, מוזיקה, ספרים ועוד, מהטלפון הוותיק אל הטלפון החדש. תהליך המעבר יתבצע במשך כ-15 דקות, ויש לוודא שהמחשב מחובר לרשת האינטרנט.

2. לאחר שהתוכנת המעבר התקנתה, יש להפעיל את הטלפון החדש ולהתחבר אליו. לאחר מכן, יש להקליק על כפתור המעבר (Transfer) ולבחור את הטלפון הוותיק. תהליך המעבר יתבצע באופן אוטומטי, ויש לוודא שהמחשב מחובר לרשת האינטרנט.

3. לאחר שהתהליך הסתיים, יש להפעיל את הטלפון החדש ולהתחבר אליו. לאחר מכן, יש להקליק על כפתור המעבר (Transfer) ולבחור את הטלפון הוותיק. תהליך המעבר יתבצע באופן אוטומטי, ויש לוודא שהמחשב מחובר לרשת האינטרנט.

4. לאחר שהתהליך הסתיים, יש להפעיל את הטלפון החדש ולהתחבר אליו. לאחר מכן, יש להקליק על כפתור המעבר (Transfer) ולבחור את הטלפון הוותיק. תהליך המעבר יתבצע באופן אוטומטי, ויש לוודא שהמחשב מחובר לרשת האינטרנט.

התהליך יתבצע באופן אוטומטי



התהליך יתבצע באופן אוטומטי

[!התהליך יתבצע באופן אוטומטי](#)

התהליך יתבצע באופן אוטומטי, אך יש צורך בהתקנת תוכנת המעבר (Transfer) על המחשב. תוכנת המעבר תאפשר למשתמש להעביר את כל הנתונים שלו, כולל תמונות, מוזיקה, ספרים ועוד, מהטלפון הוותיק אל הטלפון החדש. תהליך המעבר יתבצע במשך כ-15 דקות, ויש לוודא שהמחשב מחובר לרשת האינטרנט.

00000000 0000 0000 00 000 000000 00000 00000 00 .00000 00000 00000000000 000000000000 00 00000 00000 00000
0000000000 0000000000 00 00000 00000 000000 000000 .0000 00000 0000000 000000 00 0000000 00 00000
.00000 000000 00 0000000 00000 00000000 00000

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

[illegible]

 **PayPal**

Loggen Sie sich in Ihr Konto ein.

E-Mail Adresse

Password

Einloggen

 **PayPal**

Log In to PayPal

Email

Password

Log In

[Forgot your password?](#)

□□□ □□ □□ □□□□□ □□□□ □□□□ - 1□□□

[illegible]



Figure 4 - Installing a Malicious Profile

Figure 4 shows the warning dialog box that appears when a user attempts to install a malicious profile. The dialog box is titled "Unsigned Profile" and contains the following text: "Installing this profile will change settings on your iPad." The user is presented with two options: "Cancel" and "Install Now". The background window shows the "Installing Profile" screen for a profile named "MarbleSecurity - Malicious". The profile is unsigned and was received on Sep 3, 2013. The user is prompted to click "More Details" for more information.

(Smishing) Phishing

Smishing is a type of phishing attack that uses text messages to trick users into providing sensitive information. The attacker sends a text message that appears to be from a legitimate source, such as a bank or a government agency, and asks the user to click on a link or provide a code. The user is then redirected to a fake website or their information is stolen. Smishing is a common type of phishing attack because it is easy to send and receive text messages. The user is often tricked into providing their phone number, email address, or other personal information. The attacker can then use this information to steal the user's identity or money. Smishing is a serious threat to personal and financial security. Users should be cautious of text messages that ask for sensitive information and should never provide it to anyone who is not a trusted contact.



Figure 5 - A Text Message Phishing Attempt

Phishing

Phishing is a type of cyber attack where the attacker tries to steal sensitive information from the user by pretending to be a legitimate entity. The attacker sends a message that appears to be from a trusted source, such as a bank or a government agency, and asks the user to provide sensitive information, such as a password or a credit card number. The user is then redirected to a fake website or their information is stolen. Phishing is a common type of cyber attack because it is easy to send and receive messages. The user is often tricked into providing their phone number, email address, or other personal information. The attacker can then use this information to steal the user's identity or money. Phishing is a serious threat to personal and financial security. Users should be cautious of messages that ask for sensitive information and should never provide it to anyone who is not a trusted contact.

: □ □ □ □ □ □

□□□□ □□□□□□

:□□□□ □□□□

□□□□□

:□□□□□□ □□□□□

05:25 - 03/07/1398

:□□□□□

□□□□□□ □□□□ - □□□□□□ □□□□□□ - □□□□□□

□□□□□

<https://www.shabakeh-mag.com/security/16063/%D9%81%DB%8C%D8%B4%DB%8C%D9%86:%D8%AF-%D8%AA%D9%84%D9%81%D9%86-%D9%87%D9%85%D8%B1%D8%A7%D9%87-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86-%D8%B1%D8%A7-%D8%B3%D8%B1%D9%82%D8%AA-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D8%AF%D8%9F>