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.

A RECENT STUDY BY FORRESTER PREDICTS THAT ONE IN FIVE U.S. ADULTS WILL DO SOME FORM OF BANKING TRANSACTION OVER THEIR MOBILE PHONES BY 2015, UP FROM THE 12% WHO CURRENTLY PERFORM SOME OF THEIR BANKING OVER MOBILE HANDSETS.

MORE THAN 6 IN 10 U.S. ADULTS (65%) CHECK SOCIAL NETWORKS ON THEIR MOBILE PHONES.

IS YOUR MOBILE PHONE SAFE?

MOBILE DEVICES ARE THE FIRST SYSTEMS TO RECEIVE FRAUDULENT EMAIL MESSAGES.

MOST FRAUDULENT EMAILS CALL FOR IMMEDIATE ACTION, SO MOBILE USERS ARE MORE LIKELY TO BE HIT BY PHISHING ATTACKS.

THE FIRST FEW HOURS ARE THE MOST IMPORTANT, BECAUSE AFTER THAT, THE SITES ARE TAKEN DOWN OR CAUGHT BY FILTERS. MOBILE USERS ARE USUALLY THE FIRST TO THE SCENE.

DID YOU KNOW...
THAT PAYMENT SERVICES ACCOUNT FOR
NEARLY 38%
OF PHISHING ATTACKS?

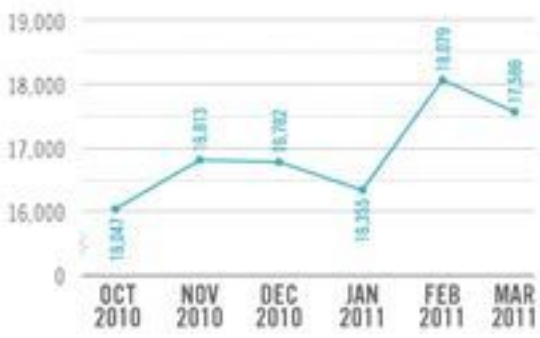
MOBILE PHISHING ATTACKS ARE MORE FREQUENT THAN YOU THINK

THE U.S. IS THE TOP COUNTRY FOR HOSTING PHISHING WEBSITES.

MOBILE USERS ACCESSING PHISHING SITES ARE 3x MORE LIKELY TO SUBMIT THEIR LOGIN INFO THAN DESKTOP USERS.

PEOPLE ARE MORE LIKELY TO SUBMIT THEIR INFO ON MOBILE THAN ON DESKTOP SITES BECAUSE IT IS HARDER TO SPOT A PHISHING WEBSITE ON A MOBILE DEVICE. FOR EXAMPLE, BLACKBERRY DOESN'T EVEN SHOW A URL BAR.

PHISHING ATTACKS PER MONTH, DEC. 2010 - MAR. 2011:



TOTAL OVER 6 MONTH PERIOD:
101,662

ANATOMY OF A PHISHING ATTACK

ATTACKERS SEND AN EMAIL THAT ASKS YOU TO UPDATE THE INFORMATION ON YOUR ACCOUNT, LIKE PAYPAL OR YOUR BANK BY VISITING A WEB PAGE.

ONCE YOU CLICK ON THE WEB PAGE, IT APPEARS LEGITIMATE, BUT UPON CLOSER INSPECTION, YOU'LL SEE THE URL IS NOT LEGITIMATE. IT MAY SAY PAYPAI INSTEAD OF PAYPAL.

THE PAGE WILL HAVE SPACES TO INPUT YOUR ACCOUNT INFORMATION AND PASSWORD. ONCE YOU DO THIS, YOUR INFORMATION GOES TO THE ATTACKERS NOT YOUR BANK.

1% OF FACEBOOK USERS HAVE BEEN VICTIMS OF PHISHING ATTACKS. WHILE THAT MAY NOT SOUND LIKE MUCH,
IT IS ACTUALLY 5 MILLION FACEBOOK USERS.

THREE BIG WAYS SCAMMERS CAN OBTAIN YOUR PERSONAL INFORMATION ON YOUR MOBILE PHONE AND HOW TO AVOID THEM

GOVERNMENT: IRS & TAX SCAMS

- A COMMON TAX PHISHING SCAM IS AN EMAIL THAT ALERTS YOU OF A PROBLEM WITH YOUR FILING REFUND. DON'T FALL FOR IT.

REMINDER: THE IRS DOES NOT USE EMAIL. IT STILL SENDS ALL CORRESPONDENCE THROUGH THE U.S. POSTAL SERVICE.

DONATIONS TO CHARITIES: JAPANESE EARTHQUAKE RELIEF

- HACKERS ARE SKILLED AT CREATING THEIR OWN FRAUDULENT DONATION SITES TO PROFIT OFF OF THE GENEROSITY OF INDIVIDUALS.

REMINDER: ON LEGITIMATE SITES SUCH AS THE RED CROSS OR DISASTER DONATE, INFORMATION SUCH AS YOUR PIN CODE, DRIVER'S LICENSE NUMBER, PHONE NUMBER OR DATE OF BIRTH IS NOT REQUIRED.

VARIOUS SOCIAL NETWORK PHISHING SCAMS

- SCAMS ON FACEBOOK, TWITTER, AND LINKEDIN CAN INCLUDE:

STEALING YOUR INFORMATION

STEALING YOUR IDENTITY

ATTACKING YOUR CONTACTS

TIPS TO STAY SAFE FROM PHISHING ON YOUR PHONE

EMAIL AND URL

- WHEN READING EMAIL OR CHECKING SOCIAL NETWORKING SITES, BE EXTRA CAUTIOUS TO LOOK AT THE SENDER OF THE EMAIL AND THE LINK THEY ARE SENDING. IF IT SEEMS OUT OF PLACE, IT PROBABLY IS.

CHECK IT TO MAKE SURE

- IF YOU HAVE ALREADY CLICKED ON A LINK, CHECK THE URL IN YOUR MOBILE BROWSER TO ENSURE IT IS A REAL WEBSITE. ANY FINANCIAL SERVICES WEBSITE THAT ASKS YOU TO INPUT YOUR ACCOUNT INFORMATION AND PASSWORD SHOULD HAVE A SECURE SYMBOL – USUALLY A LOCK IN THE ADDRESS BAR OR CHECK FOR HTTPS AT THE FRONT OF THE URL.

ANTIVIRUS AND ANTIMALWARE APPLICATION

- DOWNLOAD AN APP FOR YOUR PHONE THAT CAN CHECK EVERY WEBSITE YOU VISIT TO MAKE SURE IT'S SAFE. LOOKOUT MOBILE SECURITY HAS SAFE BROWSING BUILT INTO LOOKOUT PREMIUM AND BLOCKS PHISHING AND MALWARE SITES IN REAL-TIME.

SOURCE: emarketer.com / merkleinc.com / forrester.com

lookout
MOBILE SECURITY