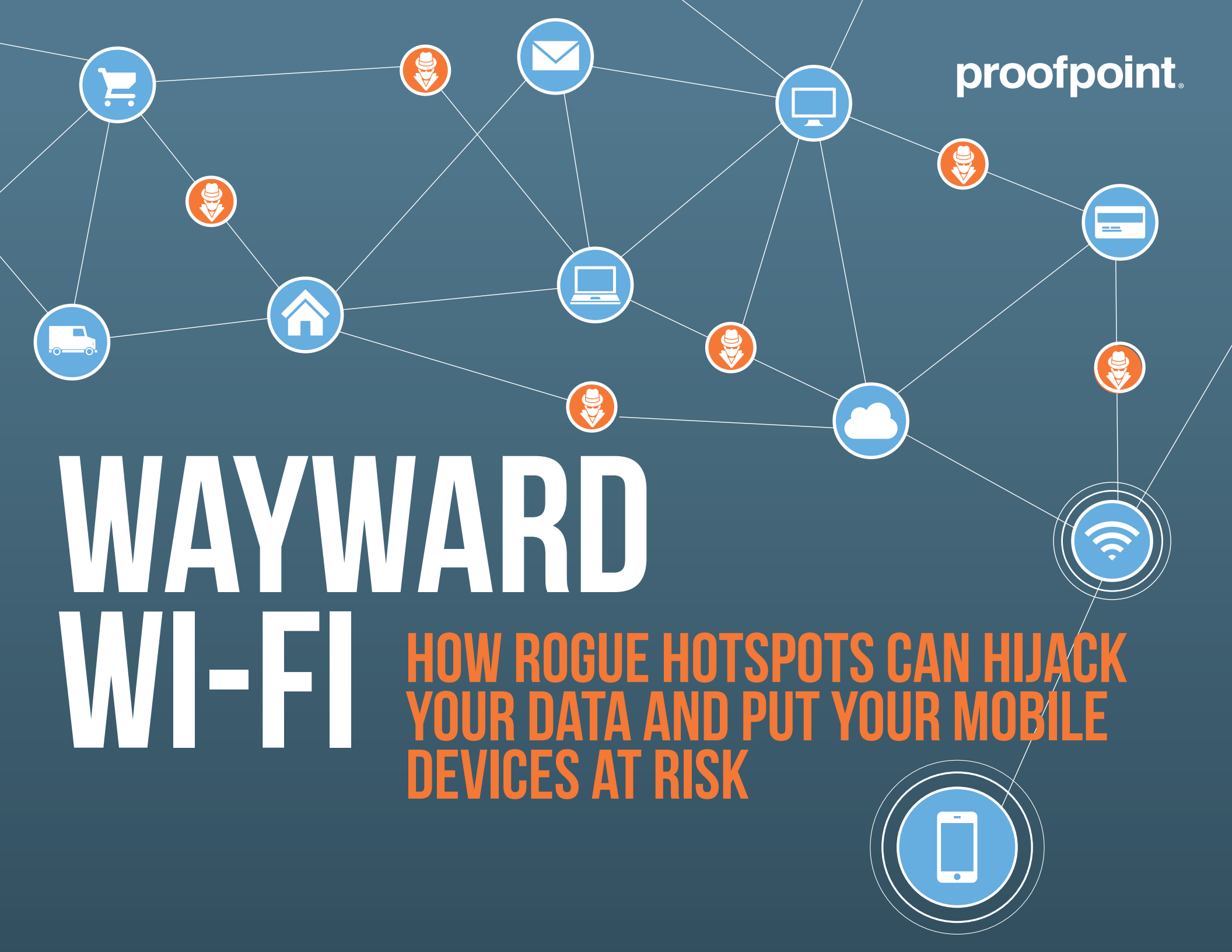


proofpoint.

WAYWARD WI-FI

HOW ROGUE HOTSPOTS CAN HIJACK YOUR DATA AND PUT YOUR MOBILE DEVICES AT RISK

288 MILLION

There are more than 288 million unique Wi-Fi networks worldwide.

Source: Wireless Geographic Logging Engine

$1.6 TRILLION

Global business travel spending will hit $1.6 trillion by 2020.

Source: Global Business Travel Association

50%

Telecommuting is becoming more common: 50% of the U.S. workforce can work remotely, and 20-25% of the workforce does so regularly.

Source: GlobalWorkplaceAnalytics.com

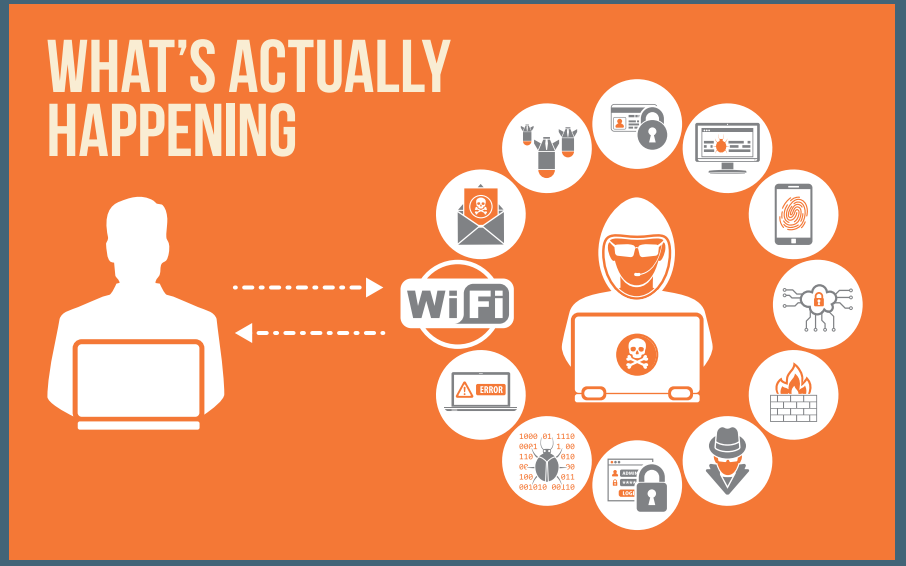
In today's digital economy, we work anywhere and everywhere. Wi-Fi networks keep us connected in airports, hotel rooms, coffee shops and remote and branch offices. But not all of those connections are what they seem. Malicious Wi-Fi networks can intercept your data—even data you think is encrypted—and put you at risk.

Cyber criminals use invisible Wi-Fi man-in-the-middle attacks to steal login credentials, identities and inflict financial disaster.

MUDDLING THE MIDDLE

In man-in-the-middle attacks, bad actors set up a malicious Wi-Fi network or take control of a compromised Wi-Fi network. When you connect to the Wi-Fi network, the attacker can see everything your computer is transmitting over Wi-Fi.

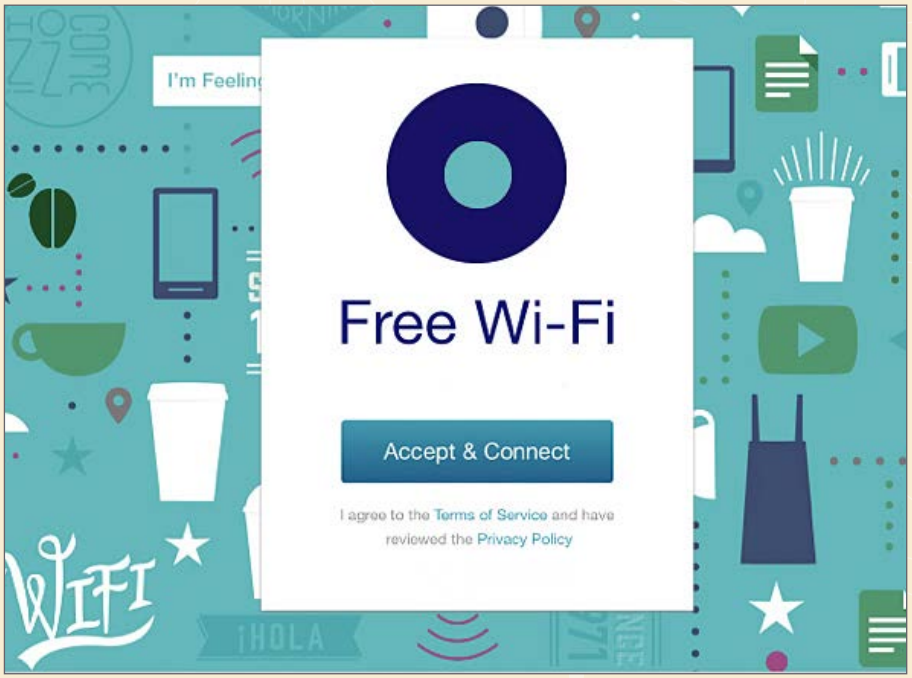
Once you've connected to the wrong Wi-Fi network, criminals can see everything, including critical passwords and all your email—even if your browsing session appears to be encrypted. These rogue networks can also even re-route your browser to data-stealing websites.



HOW ATTACKERS SET THE TRAP

Hackers create malicious Wi-Fi hotspots by using security testing tools such as $99 Wi-Fi Pineapple devices. This device creates an access point that intercepts Wi-Fi traffic to collect data and even lets attackers view your activity in real time.

Attackers give the rogue networks an innocuous-sounding name, say “FreeAirportWiFi,” to lure you into connecting. Criminals also trick you by sending a phishing email or text message with a link to a malicious website asking to “update your security settings.” When you comply, criminals are actually installing a mobile device-management profile to get access to encrypted transmissions.



TYPES OF WI-FI ATTACKS

Hotels, coffee chains and other Wi-Fi networks often redirect your web browser to a login page asking you to accept terms of usage before granting you full access to the internet. These often require you to manually click on a security certificate.

These “captive portals” are usually benign, a way for the owner of the access point to discourage abuse or display an ad.

But if you’ve connected to a malicious Wi-Fi network, attackers can create lookalike captive portals. These pages might ask you for your enterprise login credentials or credit card information.

Sometimes, even benign captive portals can be a problem. We estimate that up to 30% of free Wi-Fi networks are incorrectly configured—putting passwords, financial data and even brand reputation at risk.

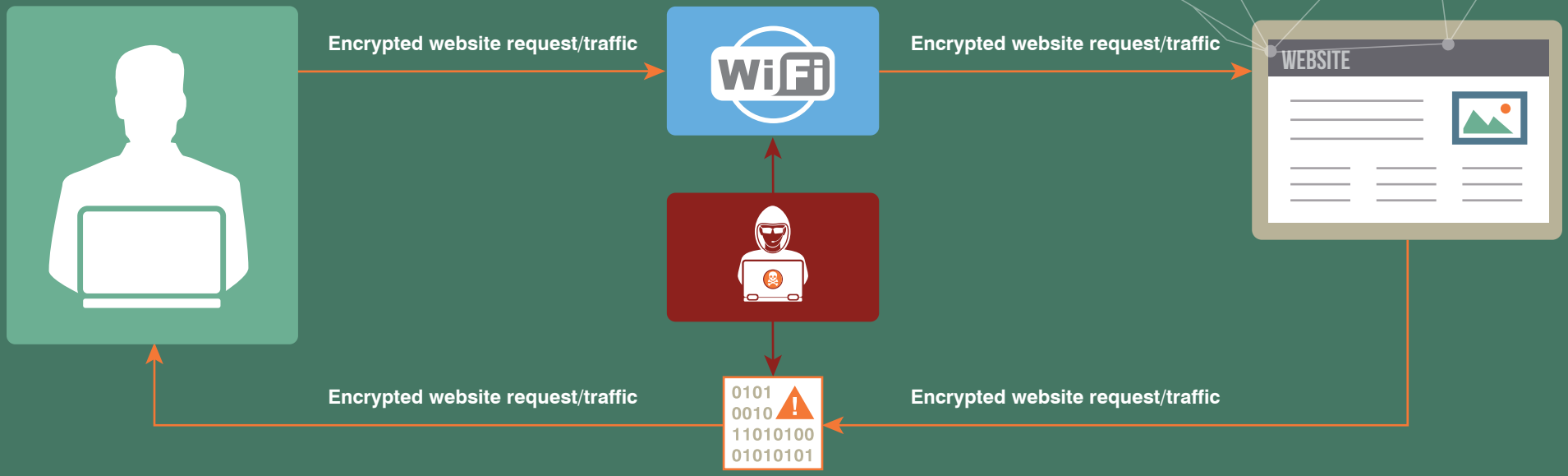
ALL WEBSITES AREN'T SAFE:

SSL SPLITTING AND STRIPPING

If you think your connection is safe because you use encrypted, think again. Attackers can silently unwrap your website requests, leaving you vulnerable.

SSL SPLITTING

During a SSL splitting attack, attackers insert themselves into the network between you and the server. That means they can see everything. The attacker unencrypts the communication between you and the websites they visit to read or capture that information. Then the attacker re-encrypts sends it on its way. Because both endpoints are expecting encrypted communication, nobody is the wiser.

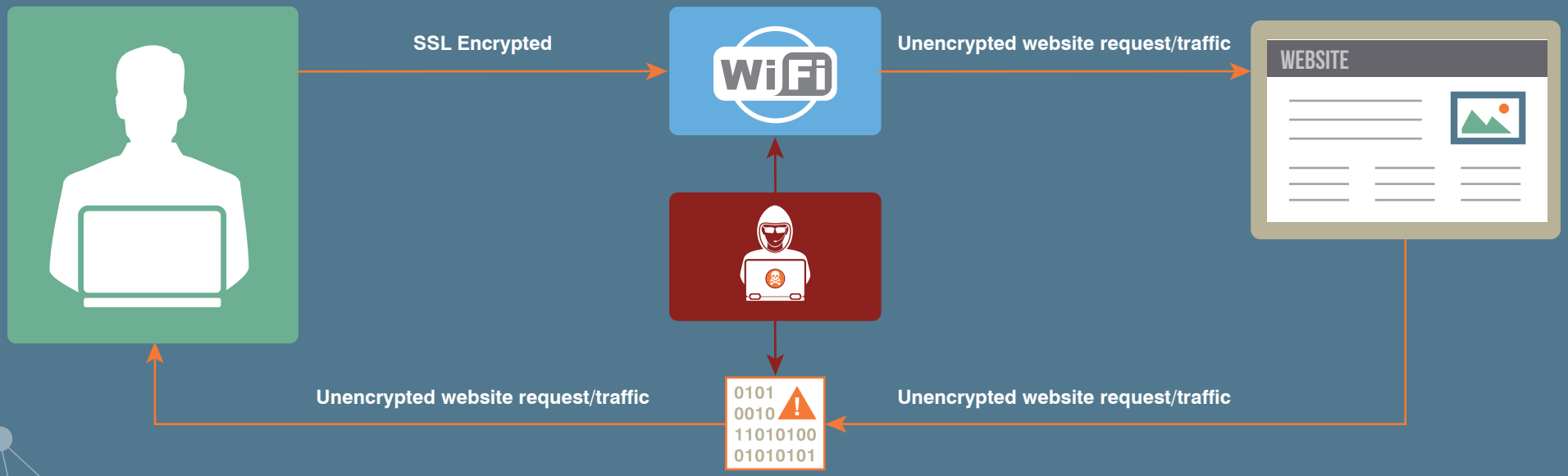


SSL STRIPPING

SSL stripping is another way to intercept encrypted communications.

In this scenario, the attacker unencrypts user communication by bouncing the web traffic from the intended encrypted (https://) site to an unencrypted site (http://). You and your mobile device are tricked into

thinking that unencrypted data is OK.

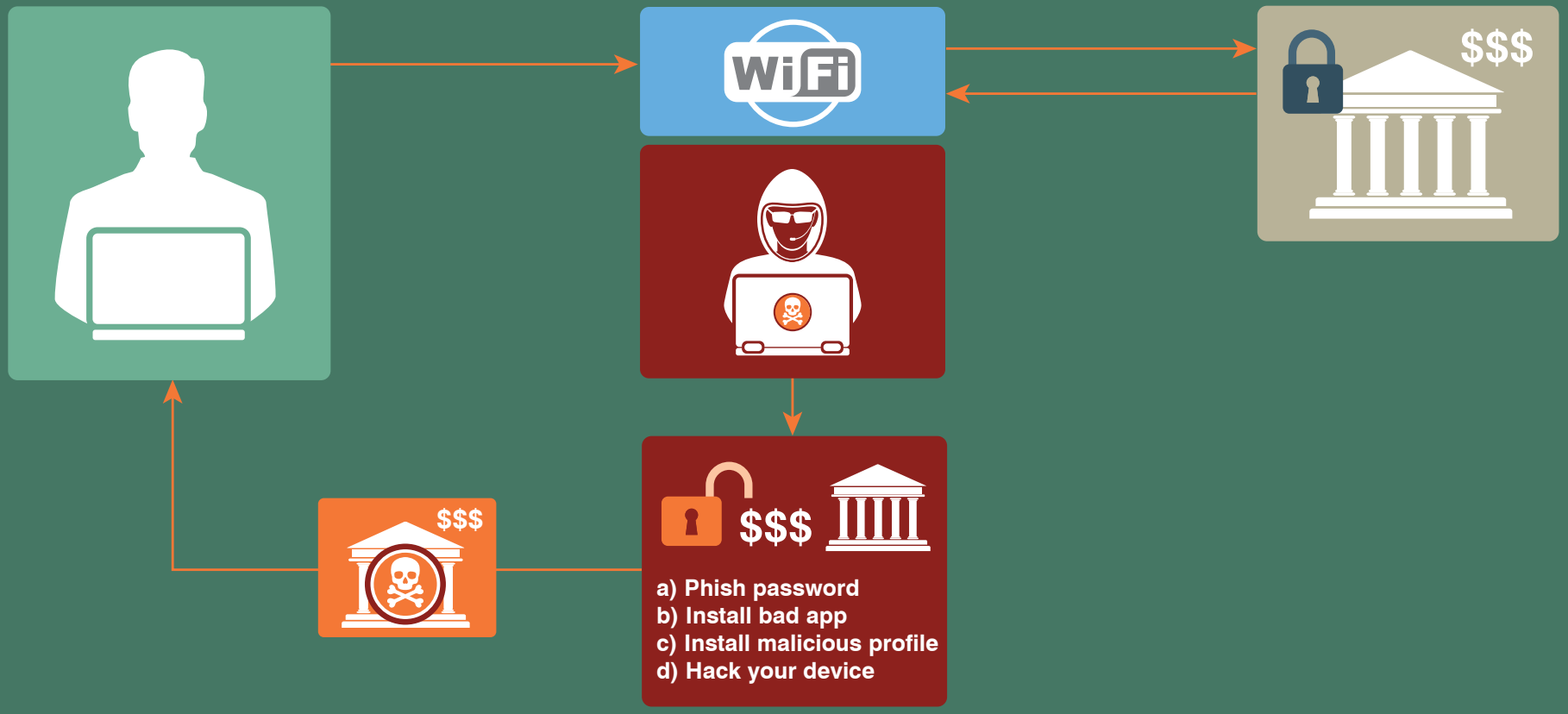


After the information is captured, there is no effort to re-encrypt the communication. So anyone on the internet can access your communication. In this case, your mobile browser will issues no warnings about certificates or security because the browser does not check for security—and the connection itself looks secure.

CONTENT MODIFICATION

Content modification occurs when the owner of the Wi-Fi access point injects additional HTML code into the wireless data stream. This code can be innocuous, such as a banner ads or alerts from the Wi-Fi provider.

But in the wrong hands, this method can let cyber criminals push malicious content or redirect you from a legitimate website to a copycat one to that pushes malware to your device or steals login credentials.



proofpoint.

HOW YOU CAN AVOID WI-FI RISKS?

Avoiding rogue Wi-Fi hotspots should be a key part of your security strategy. For information on how Proofpoint Mobile Defense protects your mobile employees from Wi-Fi attacks and warns you about risky configurations, visit

www.proofpoint.com/us/products/mobile-defense

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.