DigiKnow
CYBER SECURITY DEPENDS ON YOU

MASSIVE FACEBOOK DATA BREACH

May 2021 | Issue 2021:4

CSO's Message

Greetings,

Since the Internal Revenue Service (IRS) has extended the 2020 filing deadline until May 17, 2021, many of us are in the midst of our personal tax seasons. Things are different this year because of the Pandemic and many have questions regarding unemployment, stimulus checks and other types of financial assistance.

This uncertainty increases opportunities for cyber criminals. One of these scams is an email purportedly from the IRS with the subject "Tax Transcript" in the subject line. The email has an attachment named “Tax Account Transcript” or something similar. Don’t open this attachment. It’s malware known as Emotet that can infect your computer network and steal personal and business information.

Should you receive a suspect email the IRS urges taxpayers not to open the email or the attachment. If using a personal computer, delete or forward the scam email to phishing@irs.gov. If you see these using an employer’s computer, notify the organization's technology professionals.

The IRS will never call, email, or text you asking for your tax information. It will also not send you a message with an attachment asking you to log in to get a tax transcript or update your profile

Solomon Adote
Chief Security Officer

WHAT TO DO IF YOU ARE A VICTIM

"Business Insider," on April 3, 2021, reported a massive breach of Facebook users' data. A user in a low-level hacking forum published the phone numbers and personal data of hundreds of millions of Facebook users for free.
The exposed data includes the personal information of over 533 million Facebook users from 106 countries. This includes their phone numbers, Facebook IDs, full names, locations, birthdates, bios, and email addresses.

What do I do first? To find out if your data has been leaked we suggest using the data breach site haveibeenpwned.com. Enter your email address and/or your phone number to see if either are part of the breach. (Passwords can also be checked on this site.) So far 2.5 million email addresses were dumped, a small portion of the 553 million users who are affected.

What should I do now? In most cases, data breaches like this latest one involve less-sensitive information. If your email address was exposed, the best thing to do is to change that email account's password and set up multifactor authentication to secure it. If you find out your password was exposed, you should immediately change it on all affected accounts. If your Social Security number or other personal information was stolen, you should contact the vendor who lost it and demand free credit monitoring. You can also file a report with the appropriate government agency.

What Could Happen to My Leaked Data? Nearly 4 billion records have been stolen or accidentally leaked in the past decade, according to data collected by Privacy Rights Clearinghouse. Cybercriminals often use leaked data as a starting point for spam, phishing attacks and other forms of identity theft. Stolen records are also used for fraud, such as filing bogus unemployment claims. Other hackers use information to break into organizations' computer systems to deploy ransomware and potentially extort them.

What Else Can I Do? In addition to changing your Facebook password, now would be a good time to check your privacy settings, apps and friends, with an eye to updating and removing as appropriate. Take the time to implement two factor authentication. To activate this, go to your Facebook security settings.

Be suspect of any emails asking you to validate your account information. These phishing attempts can very accurately mimic actual financial, healthcare, and online shopping sites' logos and websites. Also be wary of emails and texts inviting you to apply for jobs that are just too good to be true. Their "job applications" are designed to extract your personal information.