pro source®
Technology Solutions

How Can Your SMB Avoid Becoming Prey?

Today's Top Cyber Criminal Strategies

TOTALPROSOURCE.COM | 888.698.0763

Introduction

Reports of massive data breaches have become commonplace, and the average cost of breaches have reached record levels. Cyber attacks are on the rise in SMBs, scams are constantly evolving, and cyber criminals are becoming increasingly savvy in using methods to get information and money from unsuspecting people. Arming yourself and your employees with knowledge on how to protect your identity is key to avoid falling victim to scammers.

Here are 7 tips to help you understand and spot today's top cyber criminal strategies.

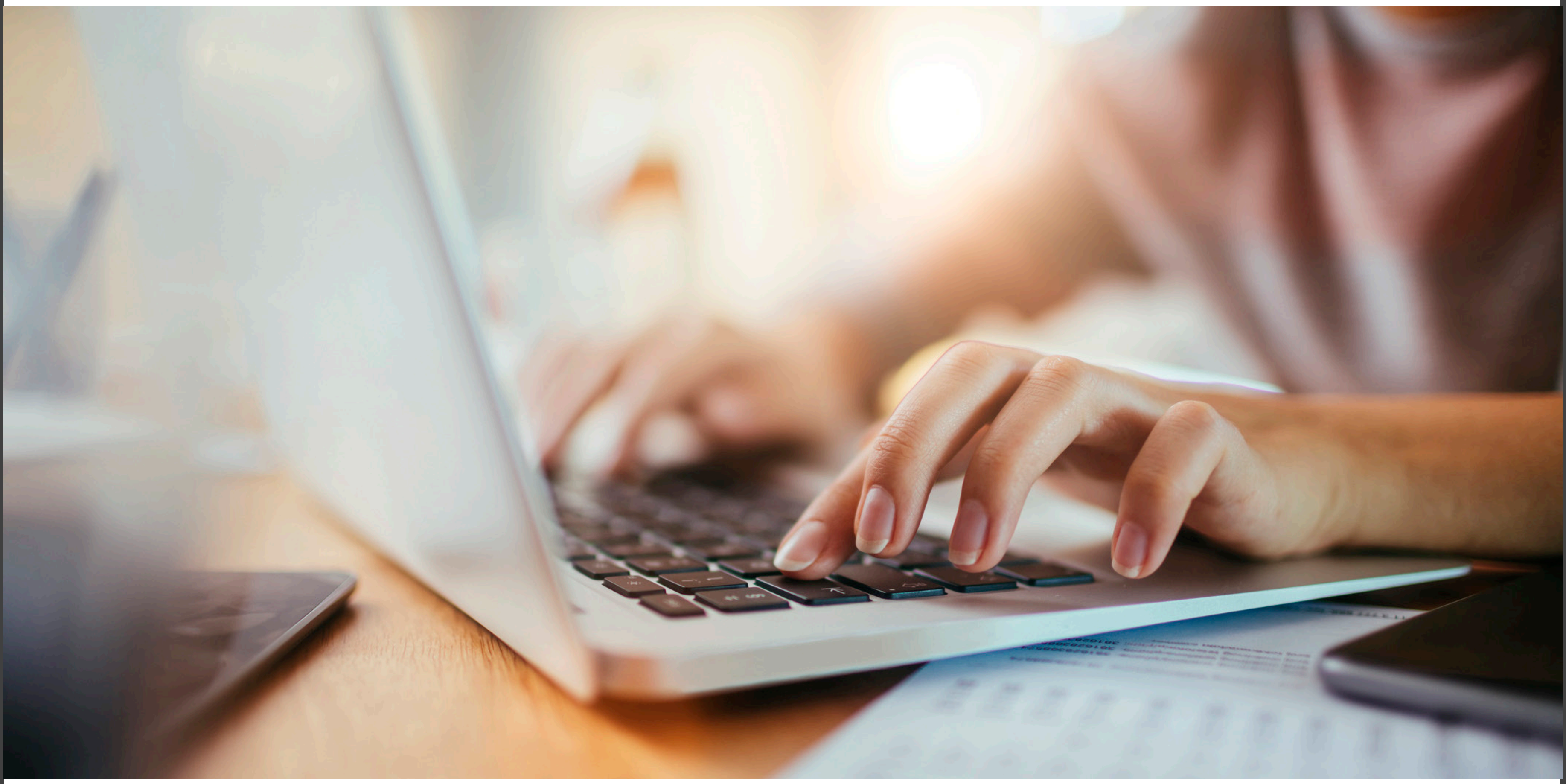
Tip #1: Phishing Attacks That Impersonate Trusted Individuals are on the Rise

Impersonation attacks are phishing attacks that imitate someone familiar, such as a co-worker, friend, or family member, to the targeted individual. These attacks are designed to steal money, intellectual property, or other sensitive data. Socially-engineered impersonation attacks are still reaching employee inboxes because commonly used systems aren't catching these threats. To ensure these types of attacks don't reach employee inboxes, it's important to implement a multi-layered approach to security.

80% increase in phishing attacks that impersonated someone familiar to the targeted individual.

Tip #2: Hackers Pose as Top Level Executives to Get Employees to Transfer Money

Spear phishers can target any one in the organization – even top executives. CEO Fraud, or fake president fraud, happens when a cyber criminal poses as a company executive and convinces an employee to send them a large sum of money. These types of attacks may vary in detail, but they all contain four major elements: the ‘president’ makes contact, the ‘president’ asks for a transfer, the ‘president’ pressures compliance, and the employee makes the transfer.



Tip 3: Top Executives are Easily Scammed by Whaling Attacks

During a whaling attack, phishers specifically target top senior management such as the CEO, CFO, or other executives who have complete access to sensitive data. The goal of a whaling attack is to trick an executive into revealing personal or corporate data, often through email and website spoofing. These attacks use fraudulent emails that appear to be from trusted sources to try to trick the victims into revealing sensitive data over email or by visiting a spoofed website. Whaling attacks are more difficult to detect than typical phishing attacks because they are highly personalized and are sent only to select targets within a company.

Tip #4: Attackers Impersonate an Individual or Organization to Send Urgent Requests and Scare the Victim into Taking Immediate Action

People are more likely to respond to a phishing email if the request is sent with a sense of urgency. Common examples of urgent requests include messages from angry bosses, late credit notices, cancelled memberships, compromised accounts, missed package deliveries, and missing rent checks. These types of emails may also be sent as requests to confirm account information or unexpected password reset requests. These messages often use the victim's name in the body of the email and are written in a stern voice to persuade victims to open attachments or reveal sensitive information.

60% of SMBs who were victims of cyber attacks did not recover and shut down within 6 months.

Tip #5: Unexpected Refunds & Payments are Hard to Resist—and Attackers Know That

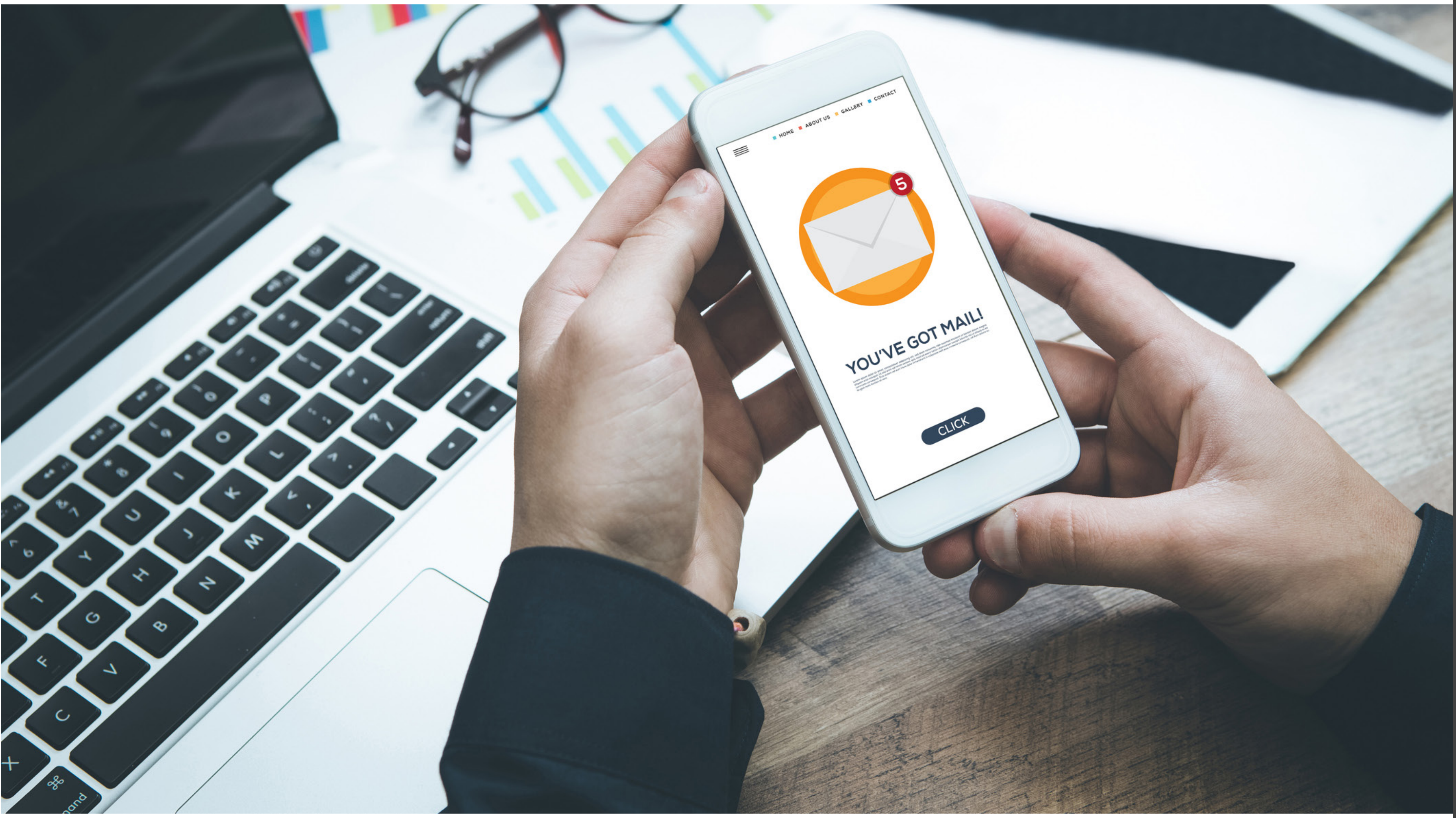
Free money and gifts are hard to resist, so it's not uncommon for phishing emails to bait victims with the promise of refunds or payments. If you receive messages claiming you are eligible for a refund or payment, it's important that you contact the business who you received this message from before doing anything. Research the company's website online and find a legitimate phone number on the website to call and validate the email. Chances are that if you receive a request for money transfers that you were previously unaware of or seem out of place, they are scam.

Tip 6: Scammers Use Unsolicited Emails Claiming You've Won a Contest to Gain Access to Information

Phishers may claim you have won or are eligible for a contest or prize even though you have not registered for a giveaway or contest. It's illegal to ask for you to pay or buy something to enter or increase your odds of winning a contest. Legitimate sweepstakes are free and by chance, so if you are asked to pay, wire money, deposit money, etc., you are receiving a contest scam.

Tip #7: Scammers are Becoming More Sophisticated with Mobile Phone Vishing

In a vishing (voice phishing) attack, scammers rely heavily on manipulation and social engineering to get victims to give personal information. Criminals typically send an email, phone message, or text pretending to be from an official source, such as a bank or government organization. The message encourages the victim to call a phone number to correct a discrepancy. Most vishing scammers now rely on “caller ID spoofing” which allows them to send out phone calls that appear to be from a legitimate or localized source. If a victim calls the number given by the scammer, they will be directed to an automated recording prompting them to provide information such as credit card numbers, birth dates, addresses, etc.



45% of organizations said phishing attempts came through phone calls or text messages

About Prosource

The rising number of mobile users, digital applications, and data networks means that individuals and businesses are becoming increasingly vulnerable to cyber exploitation. Ransomware attacks are on the rise and your data could be at risk. At Prosource, we combine products from leading cyber security and technology providers with our state-of-the-art IT services and solutions to help your business operate efficiently, effectively, and securely.

If you're interested in enhancing your cyber security efforts with a layered security approach, contact our cyber security experts by calling 888.698.0763 or by visiting totalprosource.com/contact-us.

Prosource® is one of the fastest growing companies in the Midwest with seven offices spanning across Ohio, Kentucky, Indiana, and West Virginia. Prosource provides Office Equipment, Document Automation, and Technology Solutions to businesses large and small. Founded as Cincinnati Copiers in 1985, Prosource has grown from a print and copy hardware provider to offering a full range of office technology solutions. The hallmark of Prosource's service is the TotalPro Experience, an end-to-end commitment to customer satisfaction.

pro source®

Technology Solutions

TOTALPROSOURCE.COM | 888.698.0763