SecurityAwarenessNews

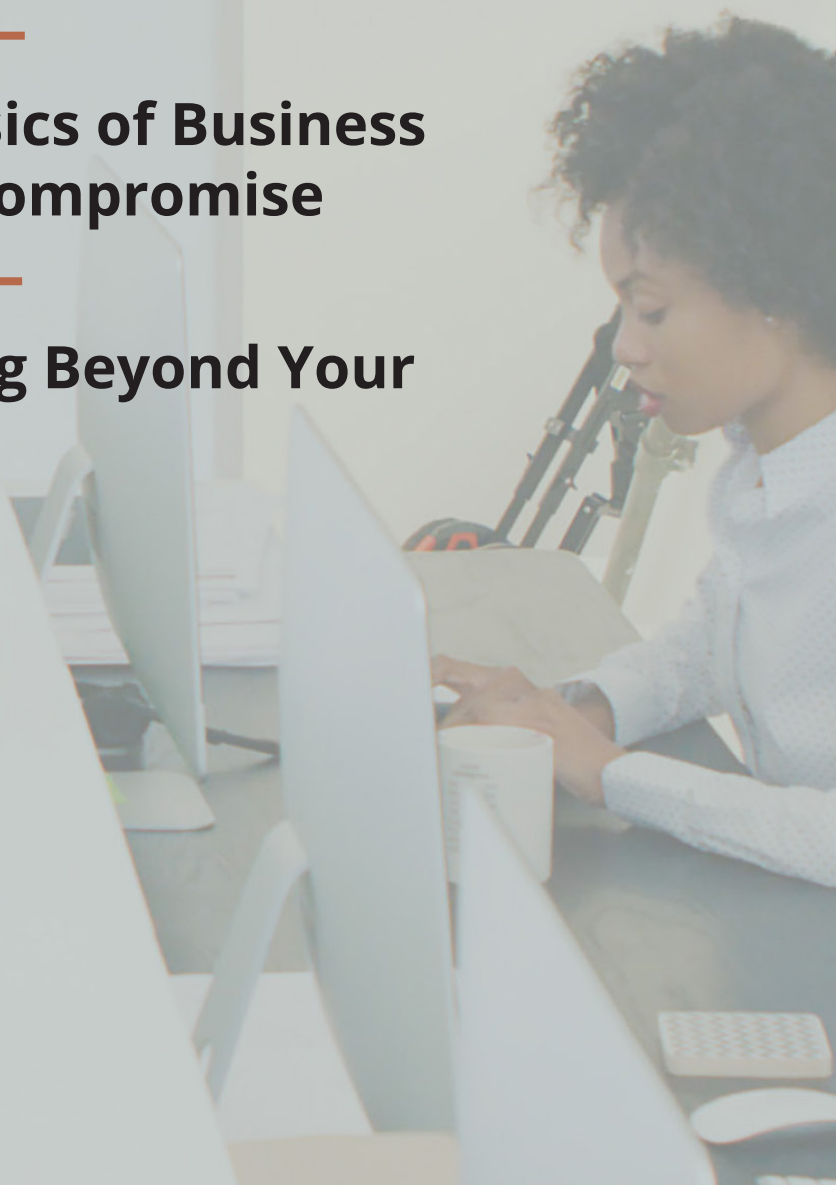
the security awareness newsletter for security aware people

Phishing Reinforcements

Identifying the Warning Signs

The Basics of Business Email Compromise

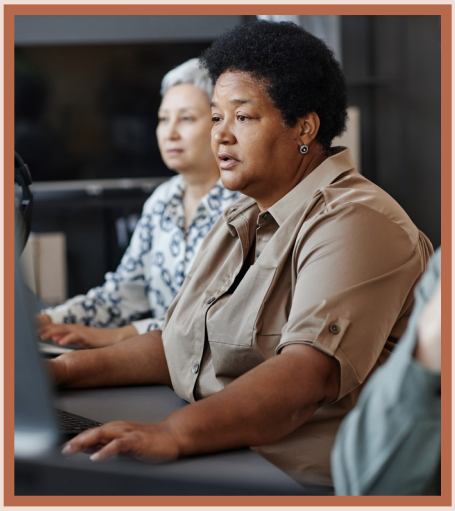
Phishing Beyond Your Inbox



Identifying the Warning Signs

Phishing is the general term given to online scams that attempt to lure people into making security mistakes. Cybercriminals use these scams to steal confidential information, steal money, and spread malware (malicious software).

While phishing attacks vary in how they target people, they usually share common warning signs that everyone should stay alert for. **Here are some of the most typical signs that you're being phished:**



Sense of urgency: An unexpected message pushes you to act "immediately," or something bad will happen.

Threatening language: The attacker may claim your bank account is locked, your payroll is paused, or that you will face legal trouble if you don't respond.

Suspicious links or attachments: Phishing messages often contain links and attachments that, if opened, can lead to malware and data theft.

Unrealistic promises: Attackers try to lure people in with "free" expensive gifts or promises of a large sum of money for little effort.

When people fail to recognize these warning signs, the outcome can be quite dangerous. Ransomware, for example, is one of the most costly. It's a type of malware that locks files or systems until a ransom is paid to restore them. But by staying alert and using security awareness, you keep yourself and your organization safe from these costly attacks.

If you encounter a phishing scam or any suspicious message, don't respond and don't open any links or attachments. Instead, report it immediately according to your organization's policies.

Timely reporting is the next most important thing to identifying attacks. It allows organizations to review what happened, spread the word to other team members of potential ongoing scams, and reduce the potential risks of something bad happening.

In summary, the best way to beat scammers is by combining three important actions:

1. Identify warning signs
2. Report anything suspicious
3. Always follow organizational policies

Those three steps help keep data, systems, and most importantly, people safe. Thanks for doing your part!

The Basics of Business Email Compromise

Many traditional phishing scams are random and unexpected. However, a more dangerous version exists called business email compromise (BEC). In this attack, a criminal does not just send a random email. Instead, they may attempt to insert themselves into a conversation you are already having. BEC often follows these phases:

The Research Phase:

Instead of sending random phishing messages, attackers will first research people on public forums such as social media. They want to find individuals who have the power to move money or have access to private data.

The Digital Break-In:

The next step is gaining access, often by stealing a real user's password. Attackers could accomplish this by sending a phishing email that directs the user to a login page that looks official but is actually a trap. Once the user enters their username and password, the attacker is in.

The Stakeout:

These scams often aim to steal large sums of money. To do that, the attacker will monitor emails and wait for a mention of a big payment or a bill.

The Hijack:

When a payment is ready, the attacker strikes. They hijack the email thread by replying with updated bank details. Since the email comes from a real, trusted account, others in the thread might not realize it is a scam.

When this scam works, money is sent directly to the criminal. These losses are often impossible to get back. And beyond losing money, a successful attack can lead to the theft of confidential information, such as your contact list and other valuable details.

Here's how you can avoid BEC scams:

Verify via a different path: If you get a request to change bank details or send data, call the person at a number you already have on file. Do not use the number in the email signature.

Question the "Why": Ask yourself why a vendor would suddenly change their payment process. Legitimate organizations rarely change bank accounts without plenty of notice.

Follow the Two-Person Rule: If your job involves moving money, always consider having a second person review and approve any changes to payment info before the money is sent.

Phishing Beyond Your Inbox

Email is not the only way scammers attempt to trick you. They will happily use any way they can to reach you. Let's explore a few other avenues where these attacks might be encountered.

Text Messages

Phishing over a text message (smishing) uses many of the same tricks as a malicious email. These messages often claim that your bank account is locked and ask you to click a link immediately. Opening the link could give a criminal access to your personal info or allow them to take over your social media accounts.

Phone Calls

Cybercriminals have been using phone calls to scam people for decades. This is often called voice phishing (vishing). Many of these attacks use automated systems that ask you to enter your bank details. Some calls will even connect you to a live scammer who pretends to be from a real company. They may try to scare you into giving them your password to "fix" a fake security problem.

Web Browsers

Have you ever seen a small pop-up message in the corner of your screen? These are called browser notifications. While some are helpful, criminal hackers use them to send fake "virus alerts" or malicious ads. These ads try to trick you into installing unwanted software. It is best to block all browser notifications to help avoid this threat.

QR Codes

QR codes are quick and easy, but they can be dangerous. Scammers use them to send you to fake websites that steal your passwords. For example, a criminal might put a fake QR code sticker over a real one on a parking meter. When you scan it to pay, you are actually sending your credit card info to a thief. Never scan a code unless you are sure it is safe.

The key takeaway: remember that phishing scams can take many forms. So stay alert and prioritize security awareness through all forms of communication.