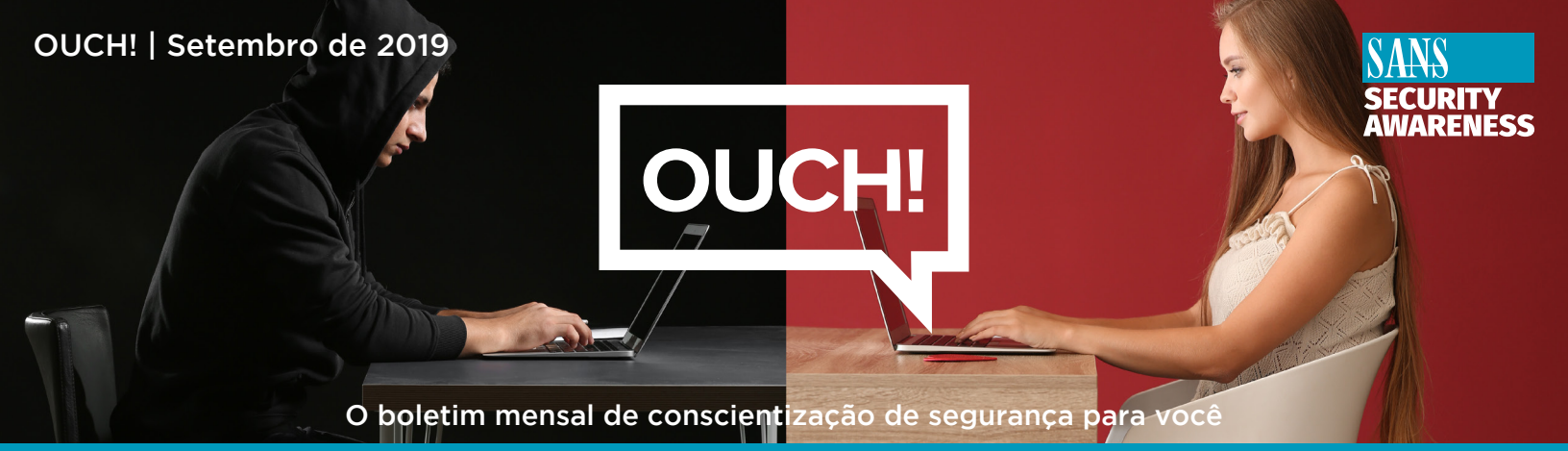

O boletim mensal de conscientização de segurança para você

Golpes através das redes sociais

Visão geral

Muitos de nós recebemos ataques por e-mail de phishing, seja no trabalho ou em casa. São e-mails que parecem legítimos, como seu banco, seu chefe ou sua loja online preferida. No entanto, esses são realmente um ataque, tentando apressá-lo ou induzi-lo a realizar uma ação que não deve executar, como abrir um anexo de e-mail infectado, compartilhar sua senha ou transferir dinheiro. O desafio é que, quanto mais experientes nos tornamos em detectar e evitar esses ataques por e-mail, mais atacantes cibernéticos tentam outras maneiras de contatar e enganar as pessoas.

Tentativas de scam ou de enganar você podem acontecer em praticamente qualquer tipo de comunicação que você usa, seja Skype, WhatsApp e Slack, Twitter, Facebook, Snapchat, Instagram ou até mesmo em aplicativos de jogos. A comunicação sobre essas plataformas ou canais pode parecer mais informal ou confiável, e é exatamente por isso que os atacantes os estão usando para enganar as outras pessoas. Além disso, com as tecnologias atuais, tornou-se muito mais fácil para qualquer invasor em qualquer lugar do mundo fingir ser qualquer pessoa ou alguém que quiser. É importante lembrar que quaisquer comunicações que surjam em seu caminho podem não ser como parecem e que as pessoas nem sempre são quem parecem ser.

Principais Conclusões

Estas são as pistas mais comuns de que a mensagem que você acabou de receber ou o post que acabou de ler pode ser um ataque.

Urgência: Uma mensagem que tem um senso de urgência que exige uma "ação imediata" antes que algo ruim aconteça, como ameaçar fechar uma conta ou mandá-lo para a cadeia. O atacante quer apressá-lo a cometer um erro.

Pressão: Pressionando você a evitar ou ignorar políticas ou procedimentos no trabalho.

Curiosidade: Um alto sentido de curiosidade ou algo que é bom demais para ser verdade. Não, você não ganhou na loteria.

Confidencial: Um pedido de informações altamente confidenciais, como seu número de cartão de crédito ou senha, ou qualquer informação que você não esteja confortável em compartilhar.

Mensagens oficiais: A mensagem diz que vem de uma organização oficial, mas tem gramática ou ortografia ruins. A maioria das organizações governamentais não usará as mídias sociais para comunicações oficiais diretamente com você. Se você não tiver certeza se a mensagem é legítima, retorne a ligação para a organização, mas use um número de telefone confiável, como um de seu site.

Roubo de identidade: Você recebe uma mensagem de um amigo ou colega de trabalho, mas o tom ou a frase simplesmente não parece ser dele. Se você suspeitar, ligue para o remetente por telefone para verificar se enviou a mensagem. É fácil para um atacante cibernético criar mensagens que pareçam ser de alguém que você conhece. Em alguns casos, eles podem assumir uma das contas de seu amigo, fingir ser seu amigo e entrar em contato com você. Fique especialmente atento a mensagens de texto, Twitter e outros formatos curtos de mensagens, o que dificulta a percepção da personalidade do remetente

Você é a melhor defesa contra golpes, desvantagens e ataques como esses. Se uma postagem ou mensagem parecer estranha ou suspeita, simplesmente ignore-a ou exclua-a ou, se for de alguém que você conhece, ligue para a pessoa e confirme se ela realmente foi enviada.

Editor convidado

Dra. Jessica Barker *(@drjessicabarker) é um líder no lado humano da segurança cibernética. Ela é co-CEO da Cygenta, onde ela segue sua paixão de influenciar positivamente a consciência, os comportamentos e a cultura de segurança cibernética em todo o mundo. Ela é a Presidente do ClubCISO e uma palestrante renomada.*

Recursos

Engenharia Social:	https://www.sans.org/u/Uz6
Golpes por chamada telefônica:	https://www.sans.org/u/Uzb
Parar esse Phish:	https://www.sans.org/u/Uzg
Golpes Personalizados:	https://www.sans.org/u/Uzl