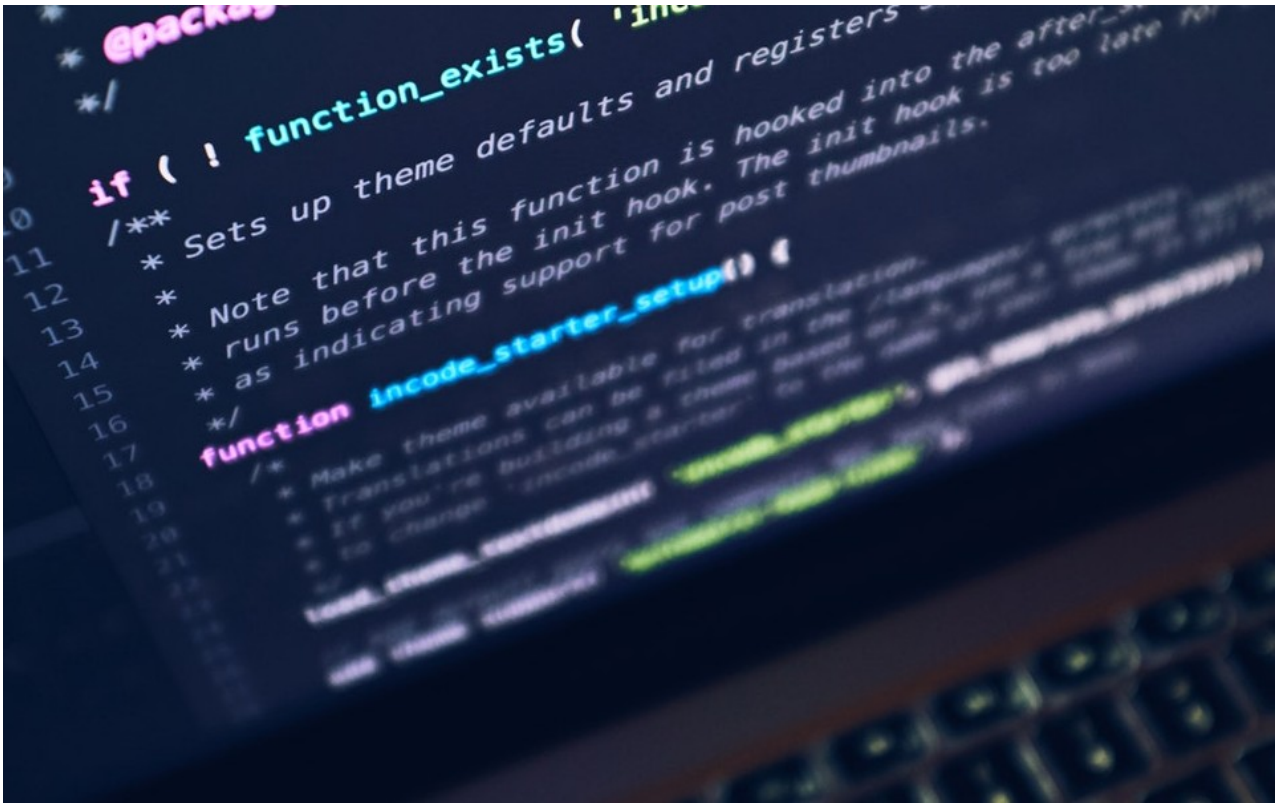
Saiba como proteger a sua organização durante a Black Friday e Cyber Monday

jornaleconomico.sapo.pt/noticias/saiba-como-proteger-a-sua-organizacao-durante-a-black-friday-e-cyber-monday-519774

29 de novembro de 2019



A Black Friday e a Cyber Monday são períodos do ano em que tanto os consumidores como as organizações estão mais expostos à burla e ao cibercrime, sobretudo desde que o comércio eletrónico se tornou um dos meios preferências de compras nestes dias de descontos invulgares.

Bruno Castro, CEO da empresa de segurança informática VisionWare, lembra que esta época começou por ser "especial", o primeiro dia seguir depois do feriado norte-americano do Dia de Ação de Graças. "Quando as lojas aproveitam para escoar stocks, oferecendo os mais variados produtos a preços bastante inferiores ao normal. O seu efeito foi sendo alargado no tempo, e muitos retalhistas – e não só – iniciam as campanhas promocionais mais cedo", recorda ao Jornal Económico.

No entanto, o risco foi-se tornando maior à medida que as montras foram sendo substituídas pelos ecrãs dos computadores e dos telemóveis – inclusive dentro de uma empresa. Tal como tem vindo a defender nos últimos anos, para a VisionWare, a maior vulnerabilidade dos negócios são as pessoas.

"Por mais que se invista em tecnologia de segurança e se criem barreiras para proteger uma determinada estrutura, o perigo pode chegar a toda a organização através de um inocente clique de um qualquer colaborador, por exemplo, no email errado ou na SMS

que parece inócua e, até, de fonte segura, mas na realidade, transporta um ataque cibernético direcionada à pessoa em causa e à organização a que pertence", lembra.

Bruno Castro recomenda:

- Investir continuamente na formação contínua. Instruir clientes e colaboradores das regras a seguir para minimizarem a possibilidade de serem alvo de burla;
- Cumprir as boas práticas e normas de segurança, para que as suas estruturas estejam defendidas num período particularmente vulnerável;
- Monitorizar com especial atenção as suas plataformas online de venda de produtos;
- Estar preparado para responder a ataques DoS (*Denial of Service* – um ataque de "negação de serviço", na qual o hacker tenta tornar os recursos do sistema indisponíveis ou sobrecarregados) que, quando bem sucedidos, podem deixar os sites das organizações em baixo, impedindo-os de funcionar corretamente e assim, de vender produtos – podendo os clientes ser levados a obter produtos similares na concorrência ou num site clonado por um criminoso.

Aos consumidores, o CEO da empresa de segurança Porto aconselha a:

- Não abrir emails ou sms de remetentes desconhecidos, seja no contacto pessoal, seja no corporativo;
- Não clicar em links ou transferir documentos suspeitos;
- Não fazer compras em sites duvidosos, confirmando sempre o certificado SSL dos sites onde navega (identificado através do cadeado do lado esquerdo e referência HTTPS), tendo a consciência de que também estes elementos podem ser manipulados pelos criminosos;
- Verificar a informação diretamente na fonte, sem aceder ao seu conteúdo no corpo do mail recebido;
- Ser cético em relação a ofertas particularmente excecionais ou que pareçam feitas à sua medida;
- Não ceder dados pessoais, nomeadamente aqueles que sejam particularmente sensíveis e que se demonstrem desnecessários à operação de compra a efetuar.