Scam of the Week: Goodbye Windows 7, Hello Social Engineering Scams

Recently, Microsoft announced they will no longer be supporting their Windows 7 operating system. This means there will be no further updates to Windows 7. The bad guys are using this situation to their advantage. They will randomly contact you by phone, emails, or pop-ups and try to convince you to pay yearly fees, or they'll insist that they need remote access to your computer so they can install "necessary" software. You'll lose your money if you mistakenly pay the fake fees, but if you grant the scammers access to your computer, your personal information and identity are at risk.

Follow the tips below to help protect yourself from these types of scams:

- **Microsoft support does not call customers.** If anyone calls you and claims that they are from Microsoft, this is a big red flag. Hang up the phone and ignore the request. If you want to speak with a legitimate customer support agent, go to Microsoft's website and find the company's customer support phone number.
- **If a computer pop-up urgently claims that your computer needs an update to it's version of Windows 7...don't fall for it!** The bad guys add flashy pop-ups to websites to trick you into thinking your computer is at risk. Do not click on the pop-up or call any numbers that are listed. This is a scam!
- **Do not share your credit or debit card information with anyone that calls you.** Never use a debit card to make online purchases, and only give someone your credit card data when you have initiated the phone call and you're sure the number is valid.

Stop, Look, and Think. *Don't be fooled.*
The KnowBe4 Security Team
KnowBe4.com