



TREMONT
FIRST NATIONAL BANK
TREMONT • HOPEDALE • NEW HOLLAND

You have to
experience it!

Cybersecurity Tip of The Week- 12/18/17

W-2 PHISHING - IT'S BACK!

W-2 phishing season is just a few weeks away. For the past several tax seasons, cyber criminals have used sophisticated social engineering tactics to dupe hundreds of payroll and HR departments into providing W-2 data on their employees, which results in the filing of fraudulent tax returns, other identity theft cases and class-action lawsuits against the company.

These attacks are incredibly disruptive to employees, extremely expensive for employers and are completely avoidable with awareness training. The typical W-2 phishing email is spoofed to look like it is from a high-level executive and asks the employee to provide W-2 or other tax-related information either by replying to the phishing email, by sending the information to another email address, or to upload it to a server owned by the bad guys.

In many instances, the request for the information appears to be urgent, which forces the employee to act quickly. These spoofed messages can be very convincing. The emails have the email address and often contain the actual signature block of the executive that makes the employee believe that the email is authentic.

THINK BEFORE YOU CLICK