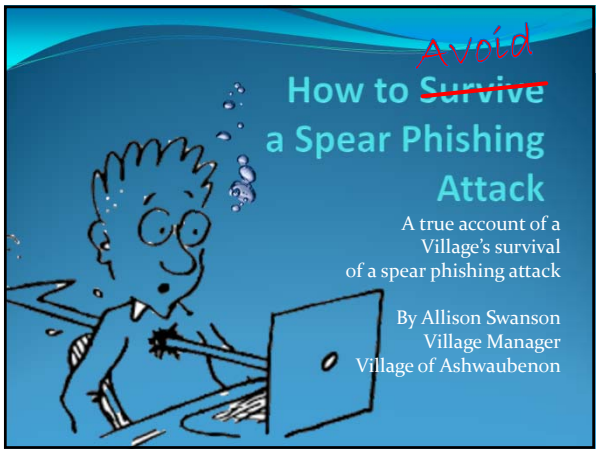
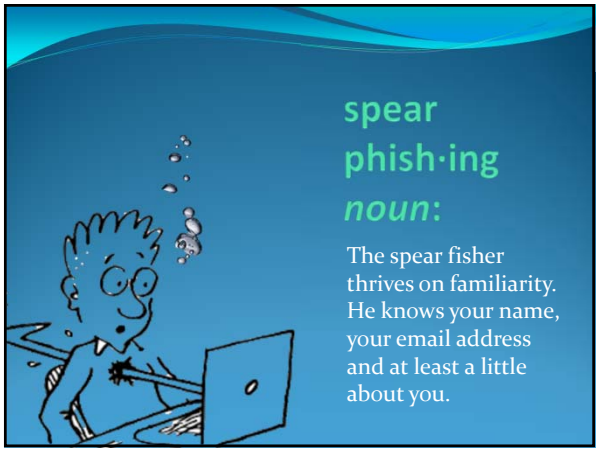

Avoid
How to Survive a Spear Phishing Attack
A true account of a Village's survival of a spear phishing attack
By Allison Swanson
Village Manager
Village of Ashwaubenon


spear phish·ing
noun:
The spear fisher thrives on familiarity. He knows your name, your email address and at least a little about you.


Powered by ThreatCloud Intelligence
THREATCLOUD
ATTACKS TODAY
WA,USA
CA,USA
AZ,USA
Finland
Romania
Russia
India
Australia
United Kingdom
South Korea
https://threatmap.checkpoint.com/ThreatPortal/livemap.html

Who is the True Vendor?

H & H Civil Construction
www.hhciveon.com

An excavating/construction firm for athletic fields and general site work

Located in Collins, a small town 30 mins. south of Green Bay & west of Manitowoc

Awarded a $2 Million contract for remediation of a park and baseball field in March 2016

Originally set up to receive paper checks in the mail for payment of invoices

How it all began: It was a dark & stormy night…

Aug. 31 – phone call

The spear phisher called our main number and asked about updating banking info for future payments

- Employee A asks caller to send her an email request to make the change

How it all began: It was a dark & stormy night…

Aug. 31 – email

- Email received from: accounts.receivable @hhcivilconstruction.com
- Email contained no name, no company logo, no phone number

How it all began:
It was a dark & stormy night…

Sept. 1 – email exchange

Employee replied to email providing a pdf of our ACH Request Form.

Spear phisher returned completed form

Employee A provides form to Employee B to complete the change in our system

Email is sent confirming change

But nothing happens…

Sept. 28 – email

- The anxious spear phisher sends an second email requesting to change their ACH info due to problems with Wells Fargo "as you have seen in the news".
- Email contained no name, no company logo, no phone number

The Saga continues…

Sept. 28 – email exchange

- Employee A forwards email to Employee B and sends form to spear phisher who again completes the form and sends it back.
- Employee B again makes changes to the vendor files.

Attack 2 is complete! The spear phisher waits…

Village is still unaware of attack…

Sept. 30 -
Employee C processes invoice for $293,310.45 submitted by the real vendor and the invoice batch is scheduled to be paid out on Oct. 3

The spear phisher waits anxiously and emails one more time on Oct. 3 to confirm that the banking info change was made…

Will the real vendor please step forward…

Oct 31 –

The real vendor contacts multiple people within the Village to ask where their payment is. Employee C tries to verify banking info and email address, but vendor states that is not correct…

Red Flags

Email contained no name, no company logo, no phone number

Phisher changes banking info twice within 30 days!

Second bank change was Sun Trust
- not located in WI
- unlikely to be used by a small company in rural WI

Had bank address been verified within info provided on the form, it would have shown that it did not match

Red Flags

Second email had a strange explanation for the change
- "Issues with Wells Fargo as you have seen in the news."

The completed ACH forms appear to have a signature of "Danielle" with no last name but printed name is Dawn Horswill; simple call or email would have shown that no such employee is at that company

Lessons Learned

Vendor file did not contain email and contact info when initially set up

Multiple vendor files for same company

No attempt to verify email address or call vendor directly

All policies needed modernization and updating in writing

Lessons Learned

Consider additional verification for high dollar transactions

Employees need more cyber training!!!

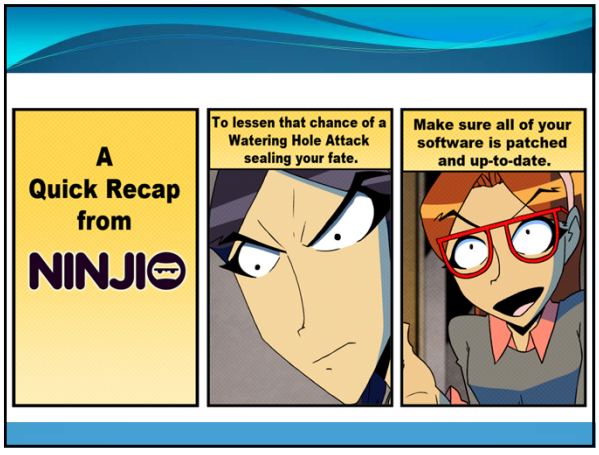
Training

Prior to the incident: all employees attended a cyber attack awareness training

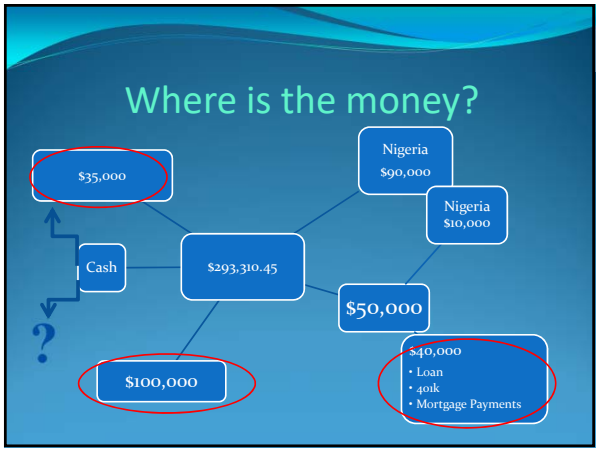
Post incident: Ninjio videos
$1.96 per employee (more than 30/less than 100 ee's)
Total cost annual cost to Village $2100

https://vimeo.com/148154237

NINJIO Season 2: Episode 1 - https://vimeo.com/196922370




FOLLOW
THE MONEY


Where is the money?
$35,000
Nigeria
$90,000
Nigeria
$10,000
Cash
$293,310.45
$50,000
?
$100,000
$40,000
• Loan
• 401k
• Mortgage Payments