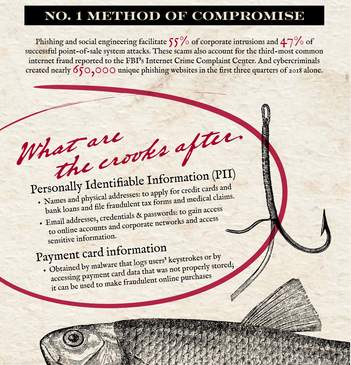
DON'T BE A PHISH OUT OF WATER

HOW TO RECOGNIZE & RESIST COMMON EMAIL CONS

phish·ing

NOUN

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, or click on malicious links and attachments.



4 HUMAN TRAITS

THAT SCAMS PREY ON

Trust
Helpfulness
Curiosity
Shame

NO. 1 METHOD OF COMPROMISE

Phishing and social engineering facilitate 55% of corporate intrusions and 47% of successful point-of-sale system attacks. These scams also account for the third-most common internet fraud reported to the FBI's Internet Crime Complaint Center. And cybercriminals created nearly 850,000 unique phishing websites in the first three quarters of 2018 alone.

What are the crooks after.

Personally Identifiable Information (PII)

- Names and physical addresses: to apply for credit cards and bank loans and file fraudulent tax forms and medical claims.
- Email addresses, credentials & passwords: to gain access to online accounts and corporate networks and access sensitive information.

Payment card information

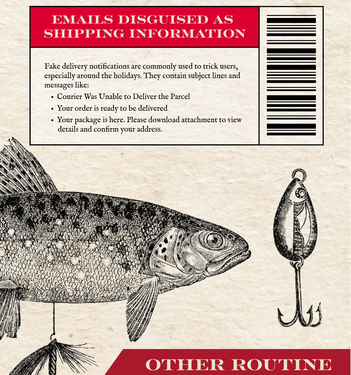
- Obtained by malware that logs users' keystrokes or by accessing payment card data that was not properly stored, it can be used to make fraudulent online purchases

Did d order something online?

EMAILS DISGUISED AS SHIPPING INFORMATION

Fake delivery notifications are commonly used to trick users, especially around the holidays. They contain subject lines and messages like:

- Courier Was Unable to Deliver the Parcel
- Your order is ready to be delivered
- Your package is here. Please download attachment to view details and confirm your address.



OTHER ROUTINE PHISHING LURES

Banks:
Fake landing page that harvests online banking credentials.

Utilities:
Fake bills from energy or telecom companies.

Finance Software:
Fake emails appearing to come from accounting providers.

Tax Returns:
Fake messages from tax collection agencies.

Mail Quota:
Fake notes warning that your mailbox is full with the goal of stealing credentials.

Popular Retailers:
Bogus receipts that lead to malicious landing pages or password reset requests with the goal of harvesting credentials. Commonly from Apple and Amazon.

Extortion:
Fake ransom notes threatening to expose supposed illicit behavior to your contact list.

CEO Fraud:
Fake or spoofed emails impersonating executives designed to trick employees into executing unauthorized wire transfers or sending tax data.

TO CATCH A PHISHER
HOW TO SPOT A SCAM

1 MISTAKEN IDENTITY
Review the sender's address and ask yourself: "Was I expecting to receive an email from this sender?"

2 THINK BEFORE YOU CLICK
Hover over links contained in the email without clicking to see where they reroute.

3 AVOID BLIND TRUST
Provide information only to websites you trust and whose address begins with "https."

4 LOST IN TRANSLATION
Watch for spelling errors and grammatical miscues, as many attacks come from non-fluent senders.

BEWARE
OF THE PDF

A hot new trend in email cybercrime involves a target receiving a message with an attached PDF file. When opened, the file displays blurred text, along with a message that the PDF is secure and must be viewed online. Clicking the link loads a URL of the attacker's choosing, leading to either a credentials-stealing page or a malware download.

1. 2018 Trustwave Global Security Report
2. Federal Bureau of Investigations Internet Crime Complaint Center 2017 Internet Crime Report
3. APWG Phishing Trend Reports