MediaPRO
Cybersecurity & Privacy Education

3 PII PHISHING TACTICS
To Look Out For

Personally identifiable information (PII) is some of the most valuable data that cybercriminals go after. With a Social Security number and birthdate, an industrious hacker could take control of nearly all aspects of your or a coworker's life.

With this much up for grabs, cybercriminals are turning to the keepers of this data—you, your employees and/or coworkers—to gain access to PII. This often means phishing emails targeted at multiple employee levels; from general employees, to middle managers, to executives.

The possibilities for phishing scams are nearly endless, but here are three examples specifically seeking PII, with advice on what to watch out for. We've broken them down by three main employee job roles often targeted by phishers:

General Employee Population

HR Managers

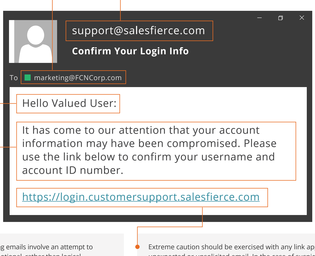
Executives

Target: General Employee Population

Almost any employee can provide an open door into an organization's network, and cybercriminals know this. Long gone are the painfully obvious "Nigerian prince" scams, replaced with cleverer and more subtle attempts, such as fake login requests meant to glean employee credentials.

Below is an example of a fake login request sent to an employee at FCN Corporation from a popular customer data management system. It asks for sensitive account information, which would potentially give the phisher access to all sorts of valuable data about FCN Corporation's customers.

- Any messages addressed generically, especially ones asking for login credentials for a specific web-based service, are suspicious.
- Watch out for mass email sends or unexpected emails to email aliases.
- Keep an eye out for "from" addresses that look odd, such as misspelled or mis-configured domain names. Phishers will often gain access to domain names that are just one letter off from legitimate ones.



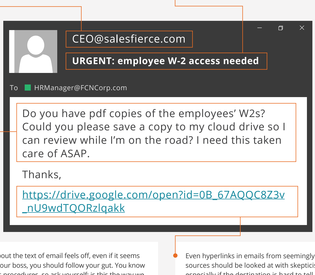
- Many phishing emails involve an attempt to trigger an emotional, rather than logical, response. Here the idea of a compromised account is meant to cause a quick, unthinking action.
- Extreme caution should be exercised with any link appearing in an unexpected or unsolicited email. In the case of suspicious looking login information requests, visit the site of the service referenced in the email directly to ensure you're logging in to the correct place.

Target: HR Managers

HR managers are in a uniquely vulnerable position when it comes to phishing emails seeking personal information, as they are often the keepers of employee tax documents, such as W-2 forms and health insurance information.

Below is an example of a phishing email spoofing a request for W-2 documents from the CEO at FCN Corporation. Read on for what signs make this email phishy.

- This email looks for all intents and purposes to be from the real CEO of FCN Corporation. However, hitting "reply" to a suspicious-looking email will usually reveal the sender's true address. Start a new email chain if you are suspicious!
- CEOs do ask for urgent requests, but it does beg the question: why does the boss need this information ASAP? Attempts like these to elicit a quick emotional response are common phishing tactics.



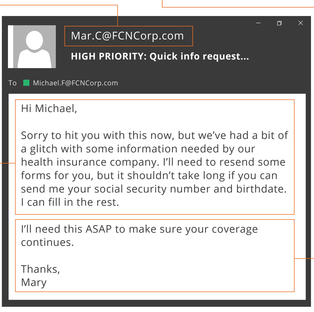
- If something about the text of email feels off, even if it seems to come from your boss, you should follow your gut. You know your company's procedures, so ask yourself: is this the way we do business? Additionally, follow up outside of email (such as a phone call) may be warranted for requests of this nature. If PII is at stake, most CEOs shouldn't mind a little due diligence.
- Even hyperlinks in emails from seemingly trusted sources should be looked at with skepticism, especially if the destination is hard to tell from the URL itself. Hover over hyperlink text (or long-press on mobile) to see where the URL would actually direct you if clicked.

Target: Executives

As the ultimate privileged users, executives and members of an organization's c-suite are increasingly becoming targets of phishing attacks. Phishers will typically craft emails tailored to executives (called spear phishing) in hopes of increasing the chances of a click. These can include malicious attachments sent for "review" or fake login requests meant to glean credentials.

Below is an example of a phishing email sent to Michael, CEO of FCN Corporation, pretending to be from FCN's own HR manager, Mary, asking to confirm some personal information.

- Display names can be spoofed by cybercriminals. Blindly hitting "reply" without taking a second look at the recipient could put sensitive PII in the hands of hackers.
- Notice the conspicuous lack of links in this particular spear phishing attempt. Some phishing emails, such as those targeting an individual, will simply request information, relying on a blind "reply" to acquire the desired data.



- If something about the text of email feels off, even if it seems to come from a trusted source, you should follow your gut. You know your company's procedures, so ask yourself: is this the way we do business? Additionally, follow up outside of email (such as a phone call) may be warranted for requests of this nature. If PII is at stake, extra precautions are warranted.

KEEPING PII SECURE

Phishing attacks that lead to a privacy breach can happen in innumerable ways. The above examples are just some of the methods cybercriminals use to collect valuable sensitive data from employees of all kinds.

Above any specific method or tactic, *all* emails requesting personal information in any form should be looked at with extra scrutiny. The reputation, financial well-being, and even the very existence of an organization can depend on it.

This advice goes for your personal life, too. You have the best understanding of what sort of emails you usually get at home and at work. If an email just feels off for any reason, that's enough to be wary of it.