

The Cybersecurity Awareness **Toolkit**

Created for Small and Medium-Sized Businesses by the National Cyber Security Alliance, Facebook and MediaPRO



Small Business Cybersecurity "Quick Wins"



Small businesses are quickly deploying various technologies to better serve their customers and manage their business more efficiently. Different kinds of technologies, however, come with a variety of risks and, thus, require alternative strategies to protect them. This "Quick Wins" sheet can be used as a starting point as a content outline for your own security awareness training program.



QUICK WINS FOR COPIER/PRINTER/FAX SECURITY.

DIGITAL COPIERS/PRINTERS/FAX MACHINES ARE COMPUTERS TOO.

- ✓ Ensure devices have encryption and overwriting
- ✓ Take advantage of all the security features offered
- ✓ Secure/wipe the hard drive before disposing of an old device
- ✓ Change the default password to a strong and unique passphrase
- ✓ Learn More: <https://www.ftc.gov/tips-advice/business-center/guidance/digital-copier-data-security-guide-businesses>



QUICK WINS FOR EMAIL SECURITY.

WHEN IN DOUBT, THROW IT OUT.

BE EXTRA CAUTIOUS WHEN IT COMES TO EMAIL.

- ✓ Require strong, unique passphrases on email accounts
- ✓ Turn on two-factor authentication
- ✓ Do not use personal email accounts for company business
- ✓ Employees should know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source. Employees should also be instructed about your company's spam filters and how to use them to prevent unwanted, harmful email
- ✓ Learn More: <https://www.ic3.gov/media/2017/170504.aspx>



QUICK WINS FOR FILE SHARING.

SHARING IS CARING, ONLY WHEN DONE SECURELY.

- ✓ Restrict the locations to which work files containing sensitive information can be saved or copied
- ✓ If possible, use application-level encryption to protect the information in your files
- ✓ Use file-naming conventions that don't disclose the types of information a file contains
- ✓ Monitor networks for sensitive information, either directly or by using a third-party service provider
- ✓ Free services do not provide the legal protection appropriate for securing sensitive information
- ✓ Learn More: <https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business>



QUICK WINS FOR MOBILE DEVICES.

KEEP A CLEAN MACHINE FOR ON-THE-GO DEVICES.

- ✓ Update security software regularly. Go ahead, update your mobile software now.
- ✓ Delete unneeded apps and update existing apps regularly
- ✓ Always download apps from a trusted source and check reviews prior to downloading
- ✓ Secure devices with passcodes or other strong authentication, such as fingerprint recognition
- ✓ Turn off Discovery Mode
- ✓ Activate "find device" and "remote wipe"
- ✓ Configure app permissions immediately after downloading
- ✓ Learn More: <https://www.stopthinkconnect.org/resources/preview/tip-sheet-stay-cyberaware-while-on-the-go-safety-tips-for-mobile-devices>



QUICK WINS FOR POINT OF SALE SYSTEMS.

HACKERS ARE OFTEN FINANCIALLY MOTIVATED.
DON'T MAKE IT AN EASY PAYDAY.

- ✓ Create unique, strong passphrases
- ✓ Separate user and administrative accounts
- ✓ Keep a clean machine: Update software regularly
- ✓ Avoid web browsing on POS terminals
- ✓ Use antivirus protection
- ✓ Learn More: <https://www.pcisecuritystandards.org/merchants/>



QUICK WINS FOR ROUTERS.

YOUR HOME OR BUSINESS NETWORK IS NOT TOO SMALL TO BE HACKED.

- ✓ Change from manufacturer's default admin password to a unique, strong passphrase
- ✓ Use a network monitoring app to scan for unwanted users
- ✓ Restrict remote administrative management
- ✓ Log out after configuring
- ✓ Keep firmware updated
- ✓ Learn More: <https://www.us-cert.gov/ncas/tips/ST15-002>



QUICK WINS FOR SOCIAL NETWORKS.

SOCIALIZE ONLINE WITH SECURITY IN MIND.

- ✓ Limit who has administrative access to your social media accounts
- ✓ Set up 2-factor authentication
- ✓ Configure your privacy settings to strengthen security and limit the amount of data shared. At the very least, review these settings annually
- ✓ Avoid third-party applications that seem suspicious and modify your settings to limit the amount of information the applications can access. Make sure you're accessing your social media accounts on a current, updated web browser
- ✓ Learn More: <https://www.us-cert.gov/ncas/tips/ST06-003>



QUICK WINS FOR SOFTWARE.

HAVING THE LATEST SECURITY SOFTWARE, WEB BROWSER AND OPERATING SYSTEM ARE THE BEST DEFENSE AGAINST THREATS.

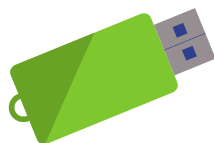
- ✓ Make sure your computer operating system, browser, and applications are set to receive automatic updates
- ✓ Ensure all software is up to date. Get rid of software you don't use
- ✓ Your company should have clear, concise rules for what employees can install and keep on their work computers
- ✓ When installing software, pay close attention to the message boxes before clicking OK, Next or I Agree
- ✓ Make sure all of your organization's computers are equipped with antivirus software and antispyware. This software should be updated regularly
- ✓ Limit access to data or systems only to those who require it to perform the core duties of their jobs
- ✓ Learn More: <https://www.lockdownyourlogin.org/update-software/>



QUICK WINS FOR THIRD PARTY VENDORS.

DO YOUR DUE DILIGENCE,
GET IT IN WRITING AND MONITOR COMPLIANCE.

- ✓ Spell out your privacy and security expectations in clear, user-friendly language to service providers
- ✓ Understand how their services work and to what you are giving them access
- ✓ Build in procedures to monitor what service providers are doing on your behalf
- ✓ Review your privacy promises from the perspective of a potential service provider
- ✓ Spell out expectations and scope of work in a formal agreement/contract
- ✓ Learn More: <https://www.ftc.gov/news-events/blogs/business-blog/2018/04/lesson-blumake-right-privacy-security-calls-when-working>



QUICK WINS FOR USB DRIVES.

THESE SMALL DEVICES CAN EASILY CREATE HUGE SECURITY ISSUES.

- ✓ Scan USBs and other external devices for viruses and malware
- ✓ Disable auto-run, which allows USB drives to open automatically when they are inserted into a drive
- ✓ Only pre-approved USB drives should be allowed in company devices. Establish policies about the use of personal, unapproved devices being plugged into work devices
- ✓ Keep personal and business USB drives separate
- ✓ Don't keep sensitive information on unencrypted USB drives. It is a good practice to keep sensitive information off of USB drives altogether
- ✓ Learn More: <https://www.us-cert.gov/ncas/tips/ST08-001>



QUICK WINS FOR WEBSITE SECURITY.

CREATE A SAFE ONLINE SHOPPING EXPERIENCE FOR YOUR CUSTOMERS.

- ✓ Keep software up-to-date
- ✓ Require users to create unique, strong passphrases to access
- ✓ Prevent direct access to upload files to your site
- ✓ Use scan tools to test your site's security - many are available free of charge
- ✓ Register sites with similar spelling to yours
- ✓ Learn More: <https://www.ftc.gov/news-events/blogs/business-blog/2018/02/hiring-web-host-ftc-has-security-tips-small-businesses>



QUICK WINS FOR WI-FI SECURITY.

THINK BEFORE YOU CONNECT.

- ✓ Use separate Wi-Fi for guests or customers than you do for business
- ✓ Physically secure Wi-Fi equipment
- ✓ Use a virtual private network (VPN) when using public Wi-Fi
- ✓ Do not connect to unknown, generic or suspicious Wi-Fi networks. Use your mobile carrier's data plan to connect instead
- ✓ Turn off Wi-Fi and Bluetooth when not in use on your devices
- ✓ Secure your internet connection by using a firewall, encrypt information and hide your Wi-Fi network
- ✓ Learn More: <https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks>

LEARN MORE ABOUT KEEPING YOUR BUSINESS SECURE
STAYSAFEONLINE.ORG/CYBERSECURE-BUSINESS

A Best Practices Guide for Comprehensive Employee Awareness Programs



Industry experts, in conjunction with MediaPRO, have compiled this extraordinarily comprehensive eBook outlining a [strategic framework](#) for successful employee awareness programs. Each section include actionable ways to improve your existing program through [analyzing](#) your unique risks, [planning](#) your program in alignment with organizational goals, [training](#) employees with engaging content, and [reinforcing](#) vital awareness principles. With guidance from this eBook, you'll be well on your way to a [NIST Cybersecurity Framework-aligned program](#) with real results.

To secure a copy of the eBook, visit the link below

<https://pages.mediapro.com/eBook-Guide-for-Comprehensive-Awareness-Programs.html>

Here's a snapshot of the content:

1. ANALYZE

A critical first step in building a risk-aware culture is knowing where you are and where you want to be. You need to assess and analyze your critical employee risks and identify behaviors that need to change in order to reduce these risks. Why deploy an awareness program if you have no way of measuring whether it's working or not?

2. PLAN

A quality awareness program plan provides you and your stakeholders with a clear roadmap for reducing risks. Using an effective planning tool, you identify behavioral risks and pinpoint the desired improvements you'll make with your awareness program. A sound plan aligns your goals with the training, reinforcement, and ongoing analytics you'll deploy to bring about the desired behavior change.

3. TRAIN

Training is the foundation of any good awareness program because it communicates desired behaviors in clearly measurable terms that ensure compliance. To get training right, you've got to deliver engaging material to the right people at the right time, with content that is entertaining, flexible, and capable of adapting to your ever-changing needs.

4. REINFORCE

While training communicates the key principles of your program, it's the way you reinforce that ensures that your message sticks with your employees. A reinforcement program that includes multi-modal content (such as animations, games, posters, articles, and more) ensures that your core InfoSec principles are embedded within your organizational culture. The best reinforcement strategies use a variety of communication methods that are aligned to support the key behavioral risks you're trying to mitigate.

3 COMMON 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.

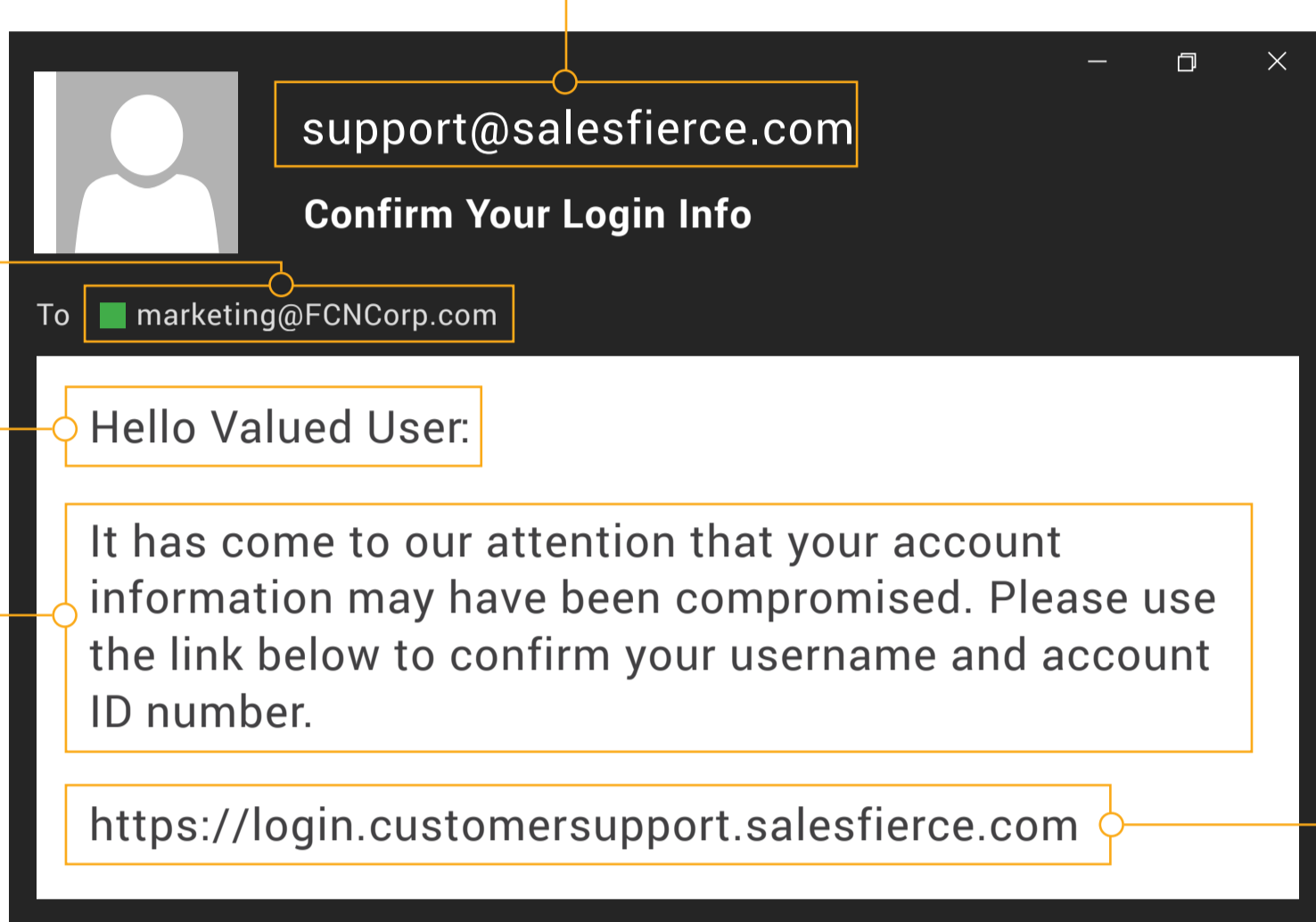
The possibilities for phishing scams are nearly endless, but here are three examples specifically seeking PII, with advice on what to watch out for. We've broken them down by three main employee job roles often targeted by phishers:

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 or 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.



Watch out for mass email sends or unexpected emails to email aliases.

Any messages addressed generically, especially ones asking for login credentials for a specific web-based service, are suspicious.

Many phishing emails involve an attempt to trigger an emotional, rather than logical, response. Here the idea of compromised account is meant to cause a quick, unthinking action.

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.

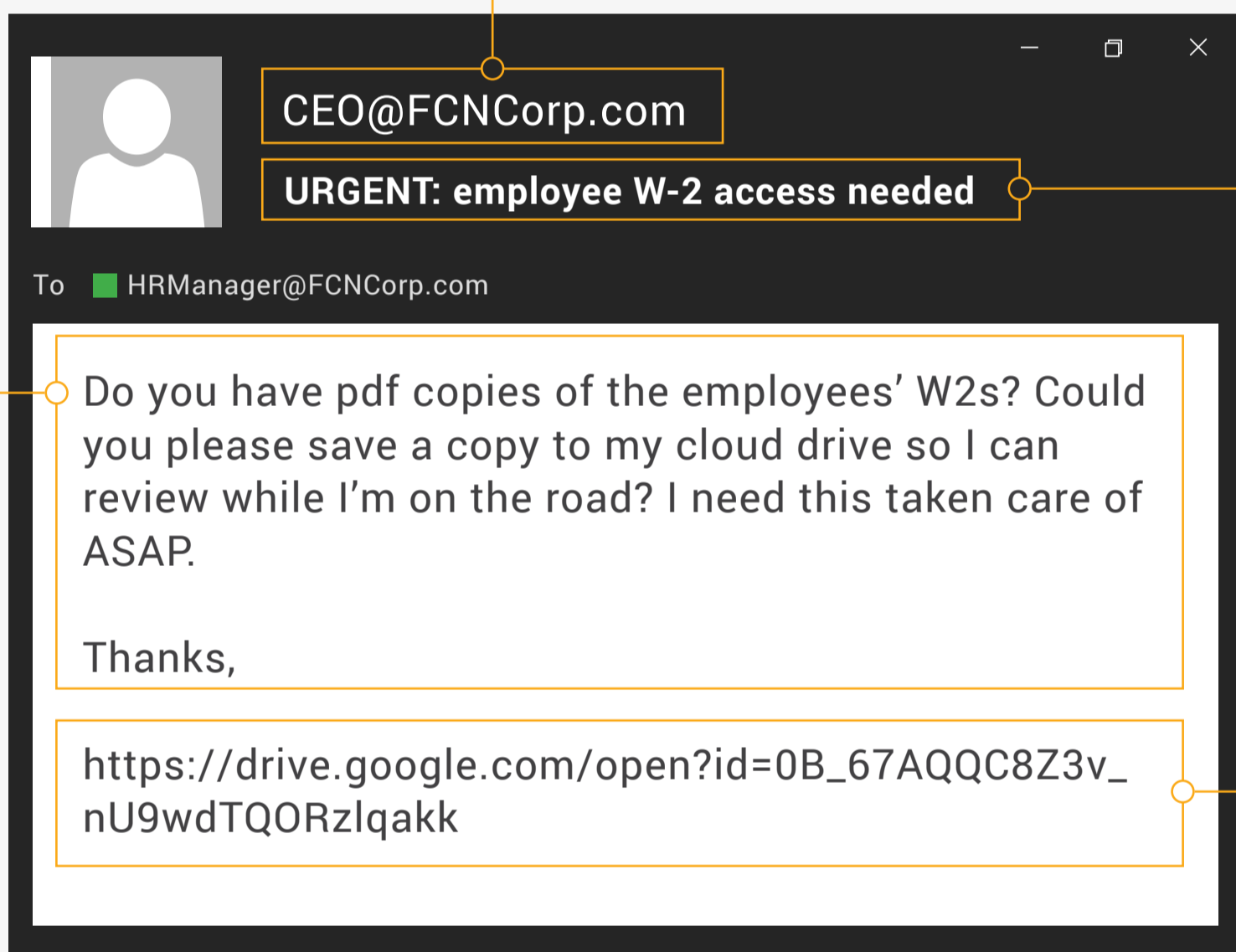
Extreme caution should be exercised with any link appearing in an unexpected or unsolicited email. In the case of suspicious looking login information requests, visit the site of the service referenced in the email directly to ensure you're logging in to the correct place.

TARGET: HUMAN RESOURCES MANAGER



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!

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.

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.

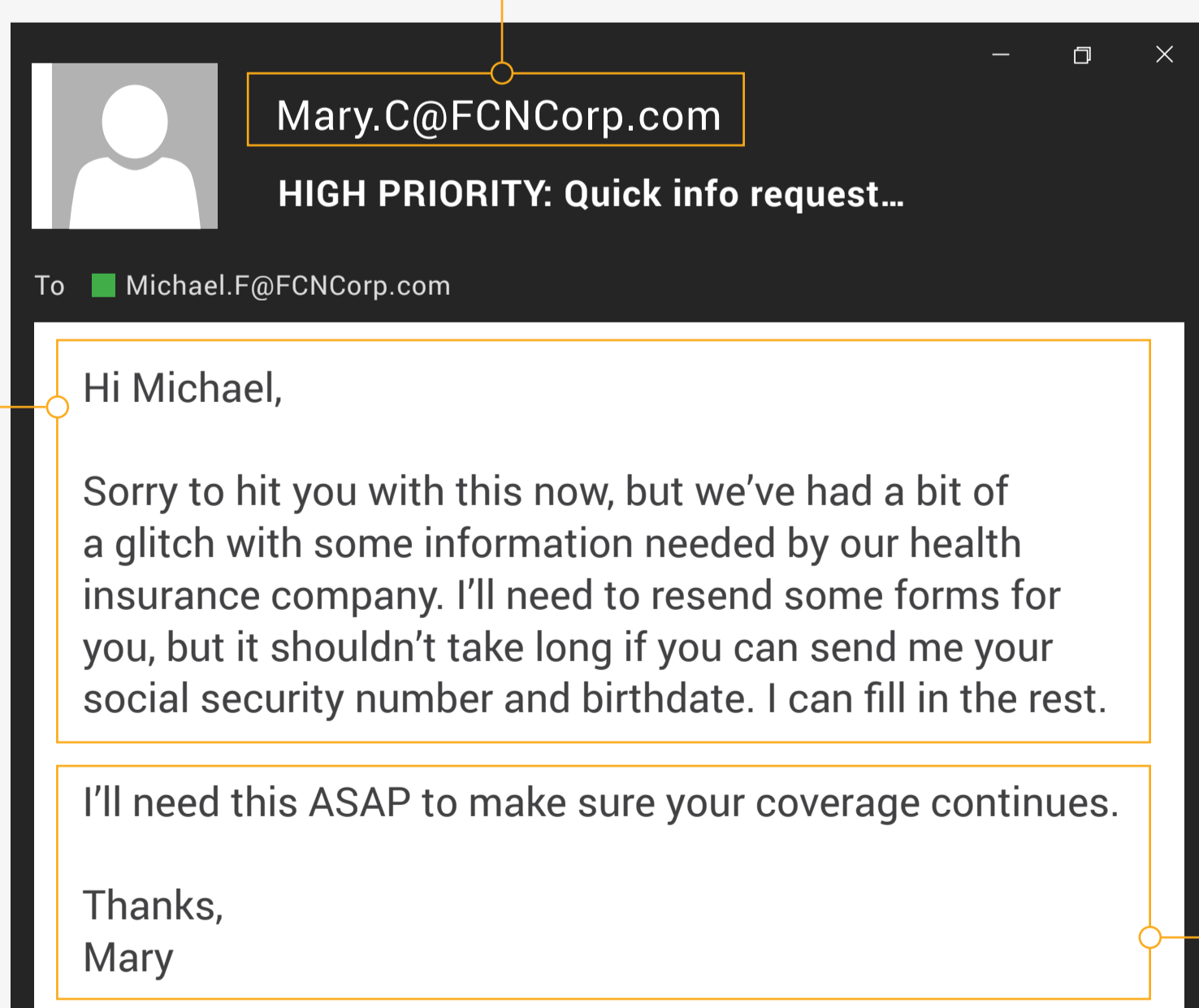
Even hyperlinks in emails from seemingly trusted sources should be looked at with skepticism, especially if the destination is hard to tell from the URL itself. Hover over hyperlink text (or long-press on mobile) to see where the URL would actually direct you if clicked.

TARGET: EXECUTIVE



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.



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.

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.

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.



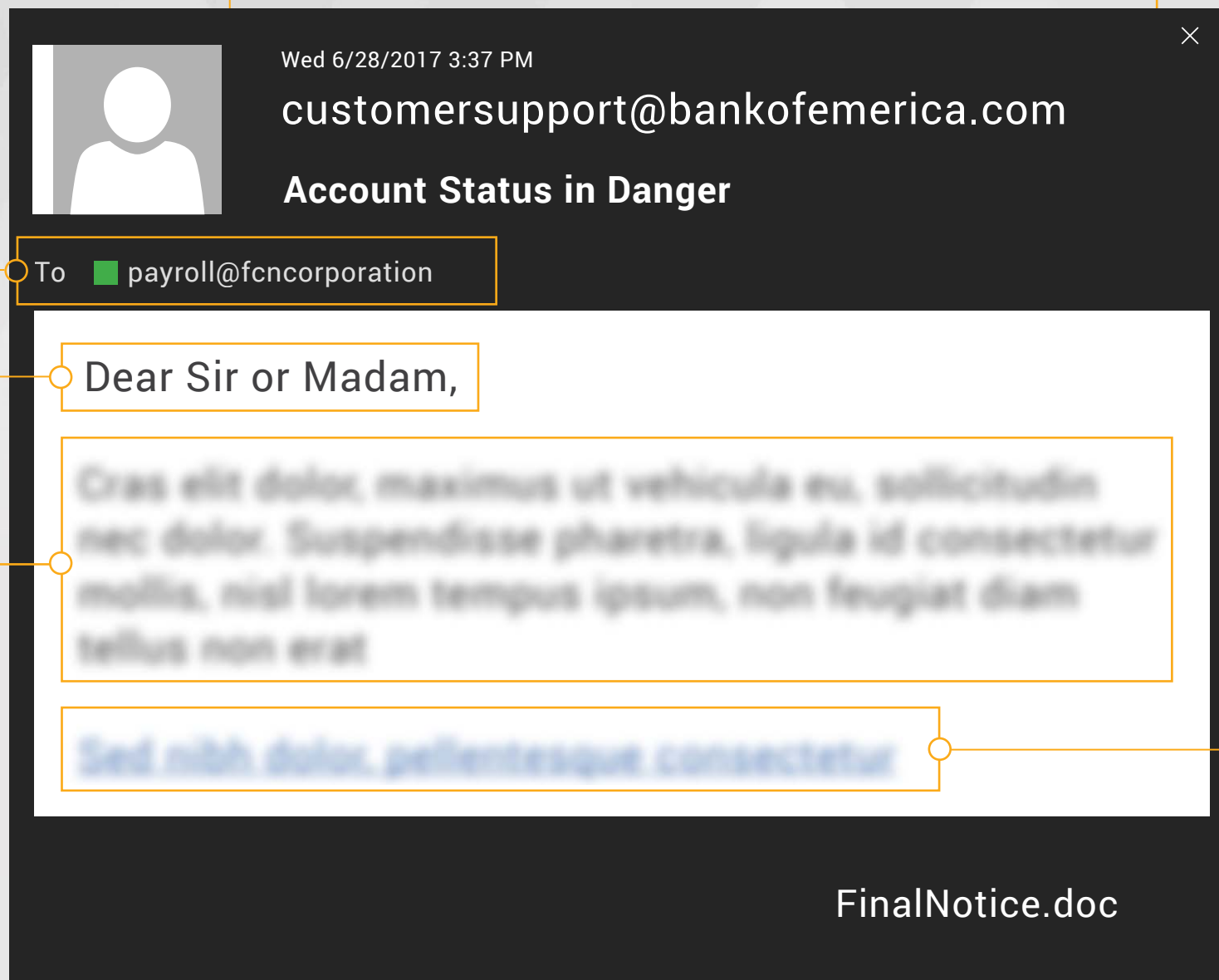
HOW TO SPOT A PHISHY EMAIL

Telltale signs to look for the next time an email that smells phishy hits your inbox

Keep an eye out for misspellings, such as legitimate business names that are missing or off by just one or two letters. Additionally, an unexpected email from an address you've never communicated with before is a good early sign of a possible scam.

Subject lines containing too-good-to-be true offers or threatening statements meant to elicit an emotional reaction are clues someone's trying to phish you.

Watch out for mass email sends or unexpected emails to email aliases, like payroll@companyxyz.



Any messages addressed generically, especially ones regarding financial transactions, are suspicious.

Extreme caution should be exercised with any link appearing in an unexpected or unsolicited email. Hover over hyperlink text (or long-press on mobile) to see where the URL would actually direct you if clicked. Scammers will also try to implant real business names in fake URLs, so be wary.

Phishing email text can take many forms, whether it's threatening legal action or telling you an unexpected package has arrived. In general, be on the lookout for:

- ✔ Demands to click
- ✔ Unreasonable free offers
- ✔ Bad grammar or misspelled words

In all circumstances: **unexpected attachments should not be opened.** Many email systems will flag or altogether block attachments for this reason. But when they don't, it's all up to the person receiving the file to decide what to do.

The You Factor

The signs above are good overall points to look for when scrutinizing a suspicious email.

However, they do not represent all the ways in which scammers will attempt to phish you or your employees. That's why a separate but vitally important way of spotting a phishing email should be pointed out. And it's sitting right where you are.

That's right, it's *you*.

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.

The sheer ingenuity of cybercriminals almost guarantees the coming years will bring phishing attempts no one has ever seen before. That's why a healthy dose of security awareness, with some skepticism and situational awareness thrown in, can go a long way.

Put these Resources into Action!

FREE CONTENT YOU CAN USE TO DESIGN YOUR OWN CYBERSECURITY AWARENESS PROGRAM

- Tips, posters and videos for kids, home, business and mobile:
 - o www.staysafeonline.org
 - o www.onguardonline.gov
- Federal Trade Commission's cybersecurity awareness publications bulk order site:
 - o www.bulkorder.ftc.gov
- Federal Inter-Agency Ransomware Guidance: How To Protect Your Networks from Ransomware:
 - o <https://www.justice.gov/criminal-ccips/file/872771/download>
- Capture the Flag:
 - o <https://github.com/facebook/fbctf>

STAY UP TO DATE ON THE LATEST SCAMS BY SIGNING UP FOR THESE ALERTS

- Federal Trade Commission Scam Alerts:
 - o www.consumer.ftc.gov/scam-alerts
- Better Business Bureau Scam Alerts:
 - o www.bbb.org/council

TEACH EMPLOYEES ABOUT STRONG AUTHENTICATION

- Lock Down Your Login's 6 simple steps to improve your online security:
 - o www.lockdownyourlogin.org
- Telesign's step-by-step instructions for enabling 2-factor authentication:
 - o www.turnon2FA.com

OTHER HELPFUL ONLINE SAFETY CONTENT

- National Cyber Security Alliance's CyberSecure My Business online resources and videos:
 - o <https://staysafeonline.org/cybersecure-business/>
- National Association of State Chief Information Officers' national map linking to each state's cybersecurity awareness website:
 - o <https://www.nascio.org/Advocacy/Cybersecurity>
- Small Business Big Threat:
 - o www.smallbusinessbigthreat.com