Monthly Cybersecurity Newsletter

January 2022 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the Interim State Chief Risk Officer – Rob Main

---

January 24-28 is Data Privacy Week!

Millions of people are unaware of and uninformed about how their personal information is used, collected, or shared online. Data Privacy Day is an international event occurring every year on January 28 to raise awareness and promote privacy and data protection best practices. In 2022, the National Cybersecurity Alliance is expanding the campaign into Data Privacy Week, a week-long initiative. Data Privacy Week helps spread awareness of online privacy and educates citizens about how to manage their personal information and keep it secure. It also encourages businesses to respect data and be more transparent about how they collect and use customer data.

The campaign focuses on raising awareness of the importance of protecting the privacy of personal information online, particularly in the context of social networking. In addition to this educational initiative, Data Privacy Week promotes events and activities that stimulate the development of technology tools that enable individual control over personally identifiable information, encourage compliance with privacy laws and regulations and create dialogue among stakeholders interested in advancing data protection and privacy.

Some examples of privacy concerns include social media sites that sell access to users through individualized advertising that puts them at risk. Many medical apps, including numerous exercise trackers and calorie counters, do not have the best security, but some fall under federal regulations that require them to safeguard their users to HIPPA standards. IDX, a provider of data breach response services, shares the following questions to ask before giving a site or app your information:

- Does the privacy policy specify what data the company or app compiles? Is it only what you choose to give it, or does it track your virtual movements even after you exit its space?
- How is the company protecting your information? What are its security measures?
- What ways is the company using your information? Does it allow you the option to specify those uses?
- Does the app ask for camera and/or location access? Does it use that access only when the app is open, or does the app track it all the time?
- Does the company give you the option to decide what cookies you allow or opt out of them altogether?
- In cases where you may be sharing medical information, is this company or app HIPPA compliant?

- Does this app come from a known source?
- Does this company offer multi-factor identification?
- Do this company allow you the option to remove your information from its database?

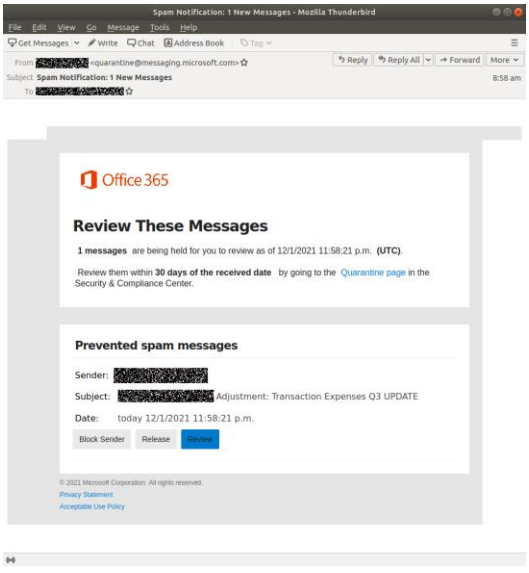
Knowing what to look for in a company, website or app is a vital part of our virtual existence. As it becomes easier to misuse personal information, asking questions like these can go a long way toward limiting exposure.

For more information about Data Privacy Week, click here.

New Office 365 "Spam Notification" Phishing Emails Seek to Capture Credentials

A new campaign spotted in the wild uses an old but effective method of convincing victims to provide their Office 365 logon credentials for use in future attacks. Security researchers at MailGuard have identified a new, realistic-looking campaign that notifies users of "spam" messages with subject lines made to look important. This technique is designed to mimic Microsoft's own security safeguards and could confuse would-be victims into trying to retrieve the nonexistent email message.

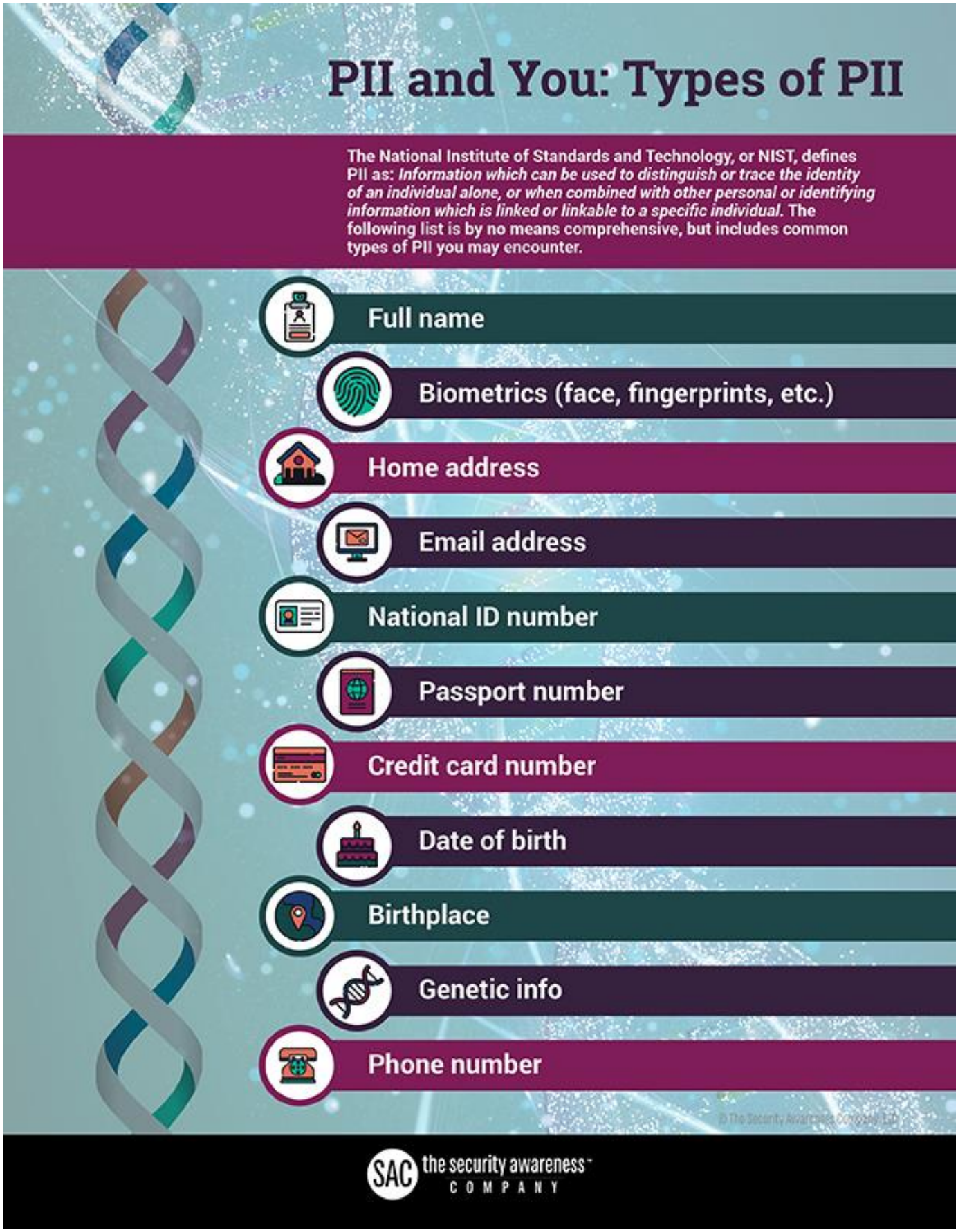
The phishing notification is convincing and impersonates Microsoft well. One small but particularly innovative feature of this phishing attempt is that the page where users are directed to provide their Office 365 credentials states "Session Expired." This makes the end user believe their O365 session has expired and establishes why the user must enter their credentials. Most attacks of this nature simply ask for credentials with no explanation why users are not taken directly to the email in question (as would be expected).



Microsoft is the most impersonated brand in phishing attacks, leveraged in nearly one-third (29%) of phishing attacks using brand impersonation. Given Microsoft's domainence of the digital world, this will likely continue for the foreseeable future. Organizations utilizing Microsoft's Office 365 services should educate users about such campaigns and use security awareness training to minimize the risk of successful attacks.

Individuals should not click links or open attachments within emails that…

- Are not addressed to you by name
- Appear to be from a legitimate company but use poor English or omit personal details that a legitimate sender would include
- Are from businesses that you were not expecting to hear from
- Take you to a page or website that is not the legitimate URL of the company the email is purporting to be sent from. Always verify the link before clicking, or better yet, go directly to the site by typing in the URL or using a pre-saved bookmark.


PII and You: Types of PII
The National Institute of Standards and Technology, or NIST, defines PII as: *Information which can be used to distinguish or trace the identity of an individual alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual.* The following list is by no means comprehensive, but includes common types of PII you may encounter.
Full name
Biometrics (face, fingerprints, etc.)
Home address
Email address
National ID number
Passport number
Credit card number
Date of birth
Birthplace
Genetic info
Phone number
SAC the security awareness COMPANY

Your customer data, intellectual property and financials are the lifeblood of your organization. If lost or leaked, there **could be significant implications for the viability of your business.** Maintaining control of that data, especially with third-party services, can be extremely challenging and requires that you ask the right questions and enforce stringent security policies.

In an environment of increased outsourcing, cloud computing adoption and regulatory requirements, **how do you manage vendor risk** and ensure you have a consistent evaluation life cycle?

In this on-demand webinar, **James McQuiggan,** KnowBe4's Security Awareness Advocate, will show you actionable steps you can use now to better manage your third-party vendor risk.

You'll learn the following:

- The importance of securing your organization's critical data
- How to determine supplier security proficiency
- The impact vendor questionnaires have on your security posture
- How leveraging a GRC platform can ease the burden of risk assessments and audits

Watch Now!

Study Shows That After a Data Breach, Users Think Changing Passwords and Good Password Hygiene Are Unimportant

New data shows that users are unconcerned after being notified of a data breach involving their credentials, personal information, and even social media accounts. A data breach is serious and only represents the beginning of what can become a sequence of malicious events involving the stolen data.

However, new data from the Identity Theft Resource Center's Data Breach Notice Research report shows that very few victims take the appropriate actions to properly secure their accounts once receiving notice of a data breach. According to the report:

- 48% only change the password for the affected account, despite 85% of respondents admitting they use the ***same password*** across multiple accounts.
- 22% changed passwords on all their accounts.
- 16% of victims take ***no action*** at all.

When asked why good password hygiene (which includes unique passwords for each account) is not being used, respondents gave the following reasons:

- 52% said it's too difficult to remember their passwords.
- 48% don't trust or know how to use password managers.
- 46% don't think it's important or believe their password practices are good enough.

These statistics indicate the necessity for proper education, so users can understand the value of unique, complex passwords and how they relate to cyberattacks in both their work and personal lives. The Identity Theft Resource Center's Data Breach Notice Research report may be found here.

FEMA's Emergency Management Institute is offering the K0428 CERT Train-the-Trainer course online, which prepares participants to deliver FEMA's CERT Basic Training course. The course dates and other course-related information are listed below.

2022 Course Dates:

- January 11, 12, 13, 18, 19 and 20 (12-4 p.m.)
- February 8, 9, 10, 15, 16 and 17 (1-5 p.m.)
- March 1, 2, 3, 8, 9 and 10 (12-4 p.m.)
- April 5, 6, 7, 12, 13and 14 (1-5 p.m.)
- June 7, 8, 9, 14, 15 and 16 (12-4 p.m.)
- July 12, 13, 14, 19, 20 and 21 (1-5 p.m.)
- September 6, 7, 8, 13, 14 and 15 (12-4 p.m.)

Class size limited to 20 students. **All times are EST**. Each course offering meets for four-hour sessions on 3 days a week for two consecutive weeks. Students must attend all sessions of their course. The audience for this course includes those who have or will have either of the following responsibilities: course manager for the CERT Basic Training course or CERT Basic Training course instructor.

These courses will be delivered in a completely virtual environment via Adobe Connect. Students should familiarize themselves with Adobe Connect. Students will use a course link to enter as guests. No Adobe Connect account or download of Adobe will be required. There is **no cost** for these courses. Students must have a FEMA student identification number, computer with microphone, speaker and stable access to the internet. Visit the FEMA Student Identification System to obtain a SID.

Prerequisites:

- A referral from a CERT-sponsoring agency, typically a local, regional or state government agency, is required.
- If you are not a first responder, the CERT Basic Training is required.
- For current first responders, IS-317: Introduction to CERT will familiarize them with the CERT Program.

Prospective students should apply through the Emergency Management Institute's online admissions system. The course offers 1.3 continuing education units. Please refer to the EMI website for course date availability.

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4.
***Note**: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2021

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/security-awareness-training/ouch-newsletter

January 18: SANS Webinar: Cloud Security for Dummies

January 18: SANS Webinar: How SMBs Can Benefit from the Security Protections of Windows 11

January 19: Info-Tech Webinar: 2022 Tech Trends

January 24-28: Data Privacy Week

January 25: SANS Webinar: Challenges Incident Response Teams Face and How to Solve Them

Also, for a list of upcoming SANS webcasts, visit here.

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember … Stop. Think. Connect.*

***Disclaimer**: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*